

Digifort Enterprise Manual
Administration Client
Version 6.4.0.0
Rev. A

Index

Part I Welcome to Digifort Enterprise Manual 10

1 Screen Shots 10
2 For whom this manual is intended 10
3 How to use this manual 10
4 Prerequisites 10

Part II Digifort Services Administrator 12

1 How to execute the Digifort Services Administrator 12
2 How to initiate the Digifort Server service 13
3 How to stop the Digifort Server service 13

Part III Basic functions of the Administration Client 15

1 How to execute the Administration Client 15
Add Server 16
Modify Server 16
Delete Server 16
Disconnect from server 16
Configurations of the Joystick 16
About Digifort 17
How to configure the servers to be administrated 17
2 How to connect a management server 18

Part IV Licensing Digifort 22

1 How to configure the licenses 22
How to add a license 24
How to send data for registration 25
How to install licenses via Online Licenses 26
How to install licenses via license files 27
Enabling a temporary license 28

Part V Registering Digifort 31

1 How to register Digifort 31
2 Registering Digifort Online 33
3 Registering Digifort Offline 34

Part VI Recording Server 37

1 How to add a camera 37
Camera data 39
Media profiles 40
How the Media Profiles save network bandwidth 41
How to add Media Profiles 42

© 2002 - 2011 by Optiview USA all rights

How to visualize the functioning of the configured media profile ... 43
Calculator for disk space usage ... 43
How to configure the recording of the camera ... 47
Camera address ... 48
Port ... 48
User and Password ... 48
Connection timeout (in MS) ... 48
Type of recording ... 48
Media profile ... 48
Motion detection ... 49
How to configure the visualization of the camera ... 49
This camera will be accessed by the client via relay server ... 50
Private IP address ... 50
Private IP port ... 50
Public IP address ... 50
Public IP port ... 50
User and Password ... 50
Connection timeout (in MS) ... 50
Media profile ... 51
Short-cut for the camera in the client ... 51
Selection of camera in the client ... 51
How to configure PTZ ... 51
Activate the PTZ control for this camera ... 52
Use the device's PTZ features ... 52
Use the device's COM port for the system to carry out PTZ functions directly ... 52
Select the PTZ protocol ... 52
Camera ID (RS-485) ... 53
COM port of video server ... 53
Presets Control button ... 53
PTZ Patrol button ... 53
Joystick Configuration button ... 53
Open Menu Controls button ... 53
How to configure the Presets Control ... 53
How to create a preset ... 55
How to configure PTZ Patrol ... 56
How to add a PTZ Patrol scheme ... 57
How to configure the scheduling of PTZ Patrol schemes ... 59
How to configure the Joystick ... 59
How to remotely configure analogical cameras ... 61
Visual joystick ... 62
Advanced PTZ ... 63
How to configure the I/O ... 65
How to add input events ... 66
How to add output events ... 68
How to configure schedulings ... 70
How to configure the scheduling of recording ... 70
How to configure the scheduling of transmission ... 72
How to configure the scheduling of events ... 73
How to configure the Motion Sensor ... 74
How to configure the recording visualization rights ... 77
How to configure the live visualization rights ... 79
How to configure the Image Buffer ... 81
How to configure camera events ... 82

© 2002 - 2011 by Optiview USA all rights

How to configure automatic events ... 83
How to configure the communications failure event ... 84
How to configure the recording failure event ... 84
How to configure the motion detection event ... 85
How to configure the manual events ... 85
How to configure the alarm actions ... 86
Send an e-mail message to a group of persons in the case of an alarm ... 87
Display camera images in the screen of the operator ... 88
Sound an alarm in the Surveillance Client ... 89
Send instant message to the operator of the computer ... 90
Request written confirmation from users ... 91
Activate camera presets ... 91
Activate action scripts of alarm outputs ... 92
Send a HTTP Request ... 93
Create timer events ... 94
How to configure the Privacy Mask ... 95
How to configure the Disk Management ... 97
Recording by limit of days ... 98
Recording by limit of hours ... 99
How to configure the archiving ... 99
How to configure the image effects ... 100
Camera management functions ... 101
Activate camera ... 102
Disactivate camera ... 102
Transmission scheduling ... 102
Recording scheduling ... 102
Events scheduling ... 102
Media Profiles ... 103
Recording media profile ... 103
Viewing media profile ... 103
Alarm buffer ... 103
Automatic events ... 103
Disk limit ... 103
Type of recording ... 103
Relay ... 103
Give video playback rights ... 104
Give live surveillance rights ... 104
Deny video playback rights ... 104
Deny live surveillance rights ... 104
Finding and registering cameras automatically ... 104
Registration of one device only ... 108
Registration of various devices ... 108
2 Monitoring the status of the recording server ... 110
Monitoring the status of cameras individually ... 110
Recording Connection ... 111
Connections ... 112
Input Ports ... 113
Schedulings ... 114
Disk ... 115
Part VII Alarm Devices 117
1 How to access the alarm devices register ... 117
How to add an alarm device ... 118

© 2002 - 2011 by Optiview USA all rights

Main data ... 119
I/O Control ... 120
Events ... 120
Scheduling ... 121
Management functions of the Alarm Devices ... 122

Part VIII Alerts and Events 125

1 How to access the Alerts and Events ... 125

How to configure the contacts ... 126
How to add a contact ... 127
How to configure the event logs ... 129
How to visualize the event logs ... 130
How to configure the contact groups ... 131
How to add a contact group ... 132
How to configure the event logs ... 133
Activate system logs ... 135
Logs Directory ... 135
Eliminate logs older than X days ... 135
Event log options ... 135
Alarm inputs ... 135
Failure in communication with the devices ... 136
Failure in recording ... 136
Motion detection ... 136
Manual events ... 136
Timer events ... 136
Programmed events ... 136
Global events ... 136
Eventos de analítico ... 136
LPR events ... 136
Save Configurations button ... 136
How to visualize the event logs ... 136

Part IX User administration 138

1 Administrating users ... 138

Monitoring user activity ... 139
2 Adding, modifying and excluding users ... 140

User data ... 142
Login IPs ... 143
Adding a range of access IPs ... 144
Login hours ... 145
User rights ... 145
Surveillance Client Features ... 147
PTZ ... 148
Web Customization ... 149
Groups Inquiry ... 150
Rights Inquiry ... 151
3 User administration functions ... 152

Reset password ... 153
Login IPs ... 153
Block account ... 153
Unblock account ... 153
Account expiration ... 154

© 2002 - 2011 by Optiview USA all rights

Rights ... 154
Give rights ... 154
Deny rights ... 154
Features ... 154
Web customization ... 154
4 Adding, altering and excluding Groups ... 154
Group rights ... 158
Surveillance Client Features ... 158
PTZ ... 159
Rights Inquiry ... 159
5 Integration with the Active Directory ... 159
Part X BioPass 163
1 How to install BioPass on your computer ... 163
2 How to configure the BioPass ... 163
Part XI Maps 172
1 Registration of Maps ... 172
Adding Cameras ... 176
Adding Functions to the Alarm Board ... 177
Map Links ... 180
Part XII Global Events 184
1 How to access the Global Events Register ... 184
2 How to add a global event ... 185
Main data ... 186
Rights ... 186
Part XIII Analytics 190
1 Licensing the Digifort Analytics ... 190
Understanding the distributed processing ... 191
How to start the Analytics Server ... 193
How to configure the servers to be managed ... 193
How to connect a management server ... 195
How to configure the analytics licenses ... 196
2 Analytics Server Configurations ... 199
3 Adding an analytics configuration ... 201
How to configure the Basic Analytics ... 205
How to configure the Foreign Objects module ... 208
How to configure the Missing Objects module ... 210
How to configure the Face Detection module ... 212
How to configure the Advanced Analytics ... 213
How to calibrate the analytics ... 218
How to classify objects ... 221
How to configure the Analytics' Rules ... 223
How to configure the Presence rule ... 223
How to configure the Entry rule ... 224
How to configure the Exit rule ... 225
How to configure the Appear rule ... 226

© 2002 - 2011 by Optiview USA all rights

How to configure the Disappear rule ... 227
How to configure the Stopped rule ... 228
How to configure the Loitering rule ... 229
How to configure the Direction Filter rule ... 230
How to configure the Speed Filter rule ... 231
How to configure the counters ... 233
The Analytics Advanced Options ... 238
How to configure the Camera Tampering ... 238
Cancel Camera Shaking Configuration ... 239

Part XIV License Plate Recognition 242

1 How to create a License Plate Recognition Server ... 242
How to configure your LPR server ... 243
2 Licensing the LPR ... 245
How to license the LPR Server ... 245
How to license the Carmen engine ... 249
How to license the Kapta engine ... 250
3 How to configure the License Plate recognition ... 254
Configuring the Carmen Engine ... 257
Configuring the Kapta Engine ... 260
Configuring the LPR lists ... 262
Verifying the LPR Status ... 263

Part XV Sheduled Events 268

1 Registering Sheduled Event ... 268
Adding Sheduled Event ... 269
Types of Scheduling ... 270
Only once ... 270
Daily ... 272
Weekly ... 272
Monthly ... 273

Part XVI Screenstyle Administration 276

1 How to access the screenstyle administration ... 276
How to add a screenstyle ... 277

Part XVII IP Filters 281

1 How to access IP Filters ... 281
How to add authorized IPs ... 282
How to add unauthorized IPs ... 283

Part XVIII Global Configurations 285

1 General Configurations ... 285
2 Master / Slave ... 287
3 STMP Configurations ... 287
4 Disk Limits ... 288
5 Network Units ... 290
How to add a network unit ... 291

© 2002 - 2011 by Optiview USA all rights

Part XIX Server Information 295

1 Monitoring by graphics ... 296

Part XX System Logs 299

1 How to access the system logs ... 299

2 How to visualize the event logs ... 300

Part XXI Web Server 304

1 How to access the configurations of the Web Server ... 304

Part XXII Automatic Client update 307

Part XXIII Failover 311

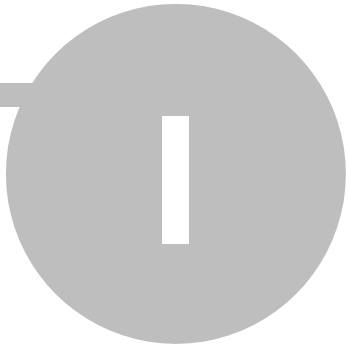
1 Configuring the Failover server ... 311

Index 0

Contact Information ... 315

© 2002 - 2011 by Optiview USA all rights

Chapter



1 Welcome to Digifort Enterprise Manual



This User Manual and Technical References provides all of the information needed to effectively implement and use all of the basic and advanced features found in the Digifort Enterprise System Administration Client.
This manual is constantly updated and does not include the features for Digifort's Beta versions. Information about the use of audio will be included in the next version of this manual.

1.1 Screen Shots

The screen shots contained in this manual may not be identical to the interface that you will see using the Administration Client. Some differences may appear, with no impairment in use of this manual. This is due to the fact that frequent updates and the inclusion of new features are carried out with the purpose of continuous improvement of the system.

1.2 For whom this manual is intended

This manual is directed toward Digifort System administrators who are responsible for the complete configuration of the Digifort Server.

1.3 How to use this manual

This manual is structured into chapters, topics, and sub-topics.
The names of the Digifort System modules and concepts involved with the system are printed in italics.
The items where the user has to interact with buttons, menus and screen names are in bold.

1.4 Prerequisites

For complete appreciation of the content of this manual, some prerequisites are necessary:

- Use of computers and their peripherals equipment.
- Use of the Microsoft Windows operating system.
- Knowledge of client-server architecture.
- Knowledge of computer network architecture.

© 2002 - 2011 by Optiview USA all rights

Chapter



2 Digifort Services Administrator

The Digifort System is a software developed around the client-server platform, making use of all the features and benefits that this platform offers.

In the client-server platform, all of the information is stored in the central server responsible for its administration. In the case of the Digifort System, the server is the component responsible for (among other functions) maintaining the recordings generated by the images supplied by cameras, administrating disk space, alerting the operators and administrators about system abnormalities and making information available to the clients.

The Digifort Server is an application that runs as a Windows system service, therefore, it is executed automatically when Windows is initiated, without need for user intervention.

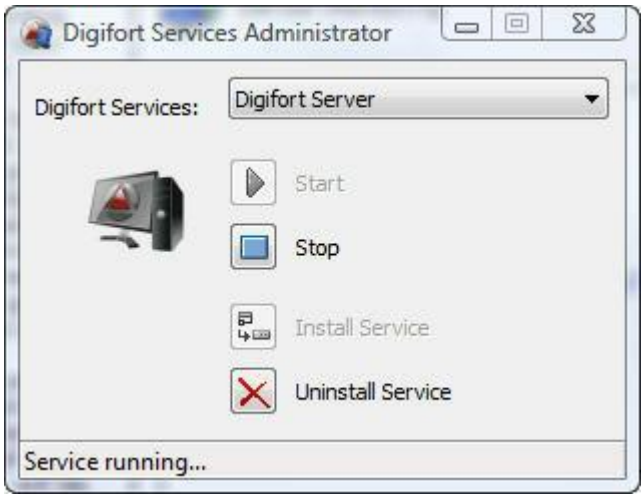
The Services Administrator is the software responsible for the control of its execution, displaying information about the state of working and offering service installation and initialization controls.

Note

As this is a Windows service, Digifort enables you to use its various features, such as the Active directory, the Explorer file management system (DHCP, UpnP), TCP/IP communication systems, video control systems, etc

2.1 How to execute the Digifort Services Administrator

To execute the Services Administrator, locate the Digifort Enterprise 6.4.0.0 Server icon on your Desktop, or, in Start->Programs->Digifort Enterprise 6.4.0.0 ->Server->Server and execute it. The Services Administrator will be started opening the screen shown in the picture below:



The Services Administrator offers the following functions:

- **Digifort Services:** Displays the list of available services that can be manipulated.
- **Initiate:** Initiates the selected service. Available only if the service is installed and stopped.

© 2002 - 2011 by Optiview USA all rights

- **Stop:** Stops the selected service. Available only if the service is installed and initiated.
- **Install Service:** Installs the selected service. Available only if the service is not installed.
- **Uninstall Service**: Uninstalls the selected service. Available only if the service is installed and stopped

2.2 How to initiate the Digifort Server service

To initiate the Digifort Server service, first it must be installed. Carry out the following steps to correctly initiate the service:

1. Select the service “Digifort Server”

2. Click on **Install Service**, a confirmation screen will be shown, informing that the service was successfully installed.

3. Click on **Initiate** and wait while the server is initiated. The process of initialization terminates when the message “Service functioning...” appears on the status bar.

Note

If the server was stopped for some reason and initiated again, the initialization process can be slow, since a check-out has to be carried out in all of the existing recordings, creating a disk structure map.

2.3 How to stop the Digifort Server service

At any moment, the execution of the Digifort Server service can be interrupted. When this is done, the server will no longer execute any function such as, for example, the administration of alarms and recording of the cameras.

The process of stopping the Digifort Server is quite simple, just clicking on the Stop button. When the service is successfully stopped, the “Service stopped...” should appear on the status bar.

© 2002 - 2011 by Optiview USA all rights

Chapter



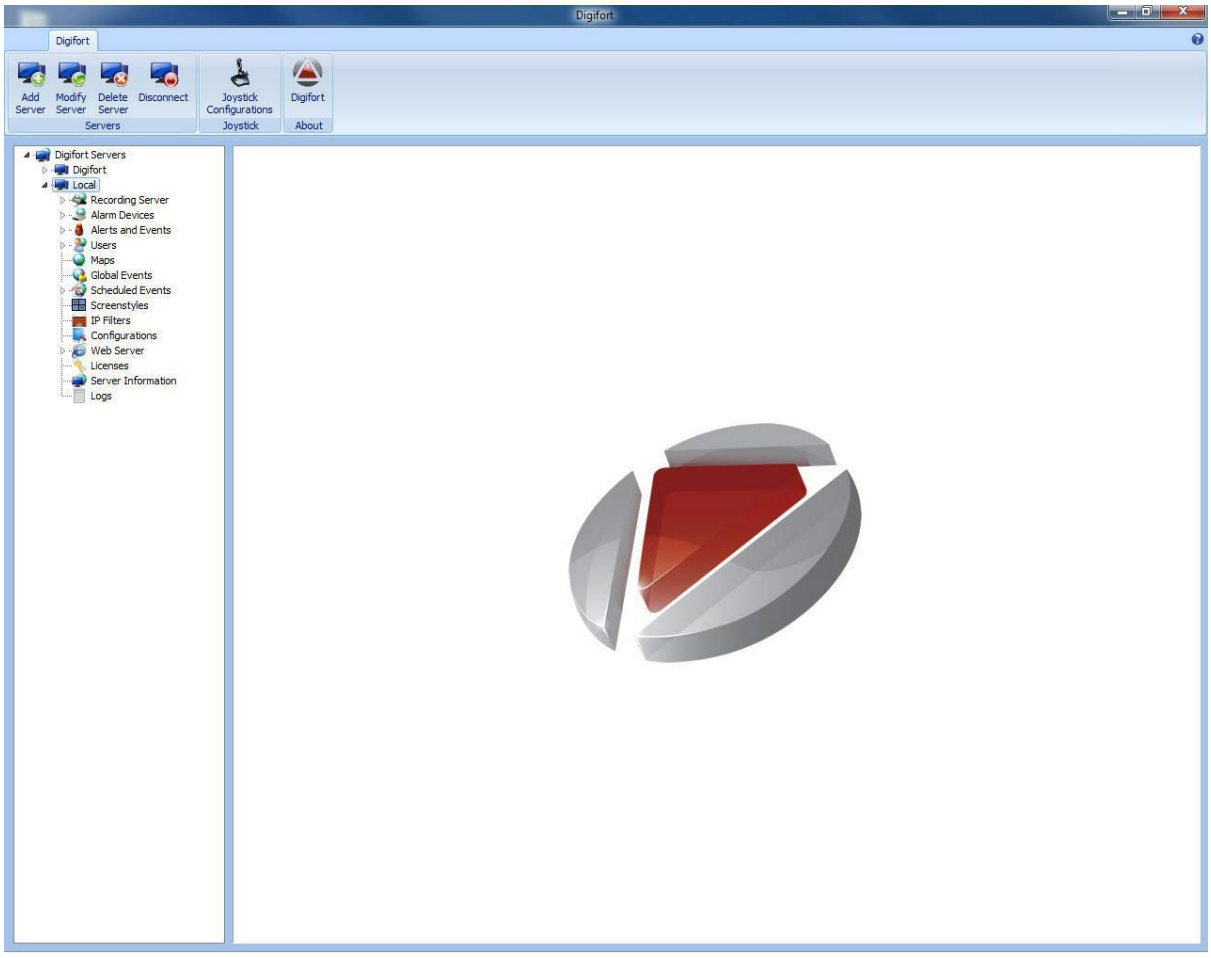
3 Basic functions of the Administration Client

The Administration Client is the Digifort System module responsible for the configuration of the server. Among other functions, in this module you can register cameras, program alarms, check the status of the server and defines the users who will have access to the system.

The Administration Client can administer an unlimited number of servers simultaneously, simply registering the desired servers.

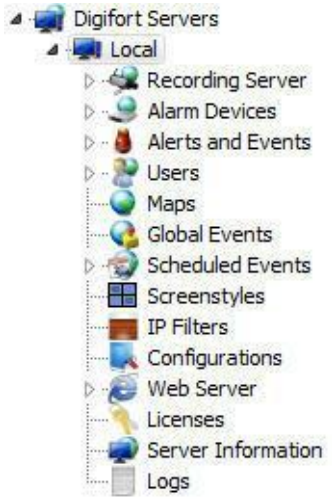
3.1 How to execute the Administration Client

To access the Administration client, locate the icon Digifort Enterprise 6.4.0.0 administration client on your Desktop or on
Start Menu->Programs->Digifort->Administration Client and run it. The Administration Client will start as shown in the figure below:



The Administration Client offers the following initial configurations:

© 2002 - 2011 by Optiview USA all rights



Configurations Menu: This menu displays the configurations available for the selected server. The configurations are shown in tree format that is, with items and sub-items. To access some server configuration, click on the desired menu. The configurations related to the selected item will be displayed in the reserved area at the right of the item.

3.1.1 Add Server



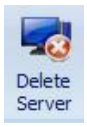
Add Server: Starts the inclusion of a server. Use this button to add servers that are administered by the Administration Client. To learn how to include servers see How to configure the servers to be administrated

3.1.2 Modify Server



Modify Server: With the server selected, this option shows the server settings configuration.

3.1.3 Delete Server



Delete Server: Delete selected server.

3.1.4 Disconnect from server



Disconnect from server: Terminates the connection and administration of the selected server. To disconnect from a server, select it in the Configurations Menu and click on this button

3.1.5 Configurations of the Joystick



Configurations of the Joystick: Open the configurations of the Joystick. To learn how to configure the joystick see How to configure the Joystick

© 2002 - 2011 by Optiview USA all rights

3.1.6 About Digifort

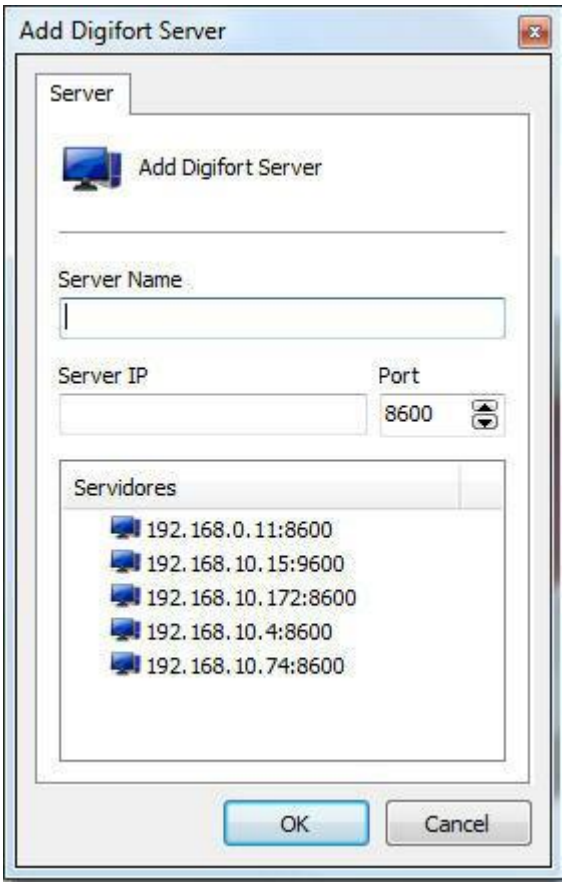


About: Show information about current Digifort version.

3.1.7 How to configure the servers to be administrated

The first step to be done in the configuration of a server is to add it to the list of servers to be administrated by the Administration Client.

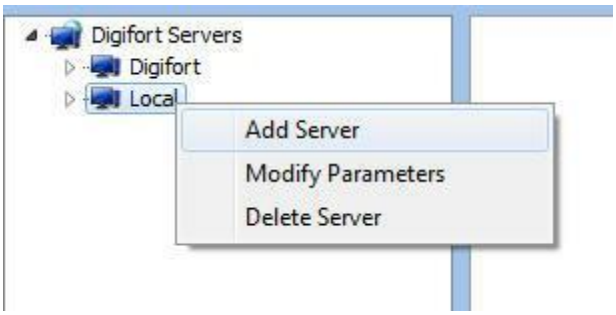
To add a server, click on the **Add** Server button, opening the server registration screen, as shown in the picture below



- **Server Name**: Enter the name of the server to be added. After confirmation of the data, the name of the server cannot be changed..
- **Server IP:** Enter the IP of the server to be administrated.
- **Port:** Enter the communication port of the server. As a standard, the port is 8600. The communication port of the server cannot be changed, this configuration should only be changed if accessing the server located in remote places, for example, Internet.
- **Servers**: This list will contain all of the Digifort servers that the Administration Client found in the network. Upon clicking on one of the servers, the IP and Port fields (described above) will be filled in automatically, leaving only the Server Name field to be entered to complete the registration.

© 2002 - 2011 by Optiview USA all rights

After correctly informing all data, click **OK**.
After inclusion of the server, it will be displayed in the Configuration Menu as shown in the picture below



To change the parameters of a server already saved, click on the right button over the desired server and then click on Modify Parameters. In the screen that opens, modify the data as necessary and click on **OK**.

To exclude a server, click on the right button over the desired server and then click on Exclude Server. Click on Yes on the confirmation message that appears.

Tip: If the Digifort Server is being executed on the same computer as the Administration Client, the Loopback IP, identified by 127.0.0.1 may be informed.

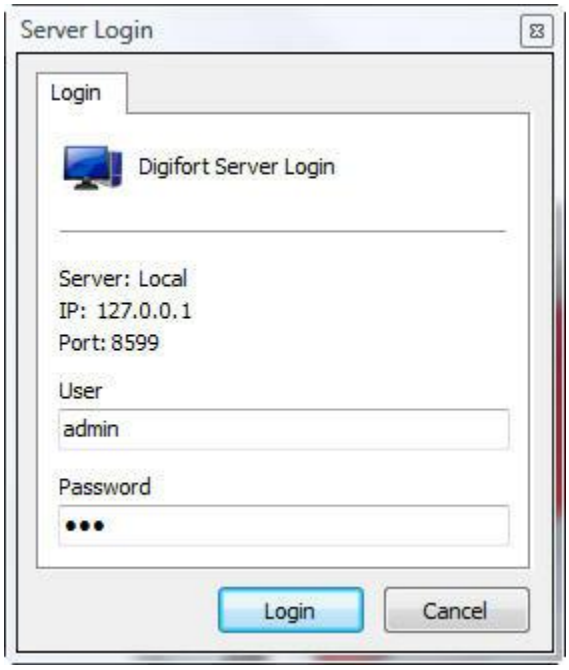
Tip

If the Digifort Server is being executed on the same computer as the Administration Client, the Loopback IP, identified by 127.0.0.1 may be informed.

3.2 How to connect a management server

After adding the server, locate in it in the Configurations Menu and double-click on it. Once this is done, you will be asked to provide a username and password to access the server configurations as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



- Username**:** Access username.
- Password**:** Password for access.

Enter your username and password to access the server. If this is the first time you are accessing the system, insert the same username as the admin and leave the password blank.

Once you have filled in the access information, click on OK. If the authentication for access is successful, the Configurations Menu opens showing the configurations available for the server, as shown in the picture below:



Note

© 2002 - 2011 by Optiview USA all rights

The admin user is the only user that cannot be removed from the system and has every right of access. For security purposes, a password must be given to stop unauthorized people accessing the system.

© 2002 - 2011 by Optiview USA all rights

Chapter IV

4 Licensing Digifort

To unblock the system, it's necessary to execute the licensing of the software.

For the Enterprise version of Digifort, a base license with support for recording of 8 initial cameras must be acquired. License packs can also be acquired, which offer support for the management of more cameras. The maximum limit for Digifort Enterprise is Unlimited.

It's important to emphasize that the licenses are only for the recording of cameras. Supposing that we have a park of 16 cameras, but have licenses for the recording of only eight. Then only eight can be recorded, the other eight can only be visualized.

The licenses only work in the server for which the registration solicitation was made. This is because each server generates a different counter-password and the licenses are granted on basis of this counter-password, making them unique.

There are two methods for licensing Digifort, licensing via Internet and via license files.
Licensing via Internet is the safest and the most recommended, but in case your server has no access to Internet, use licensing via license files.

Tip

As Digifort functions in the Client-Server platform, the registration request doesn't have to be made by the server itself, that is, any other computer in the network can make this request by way of the Administration Client.

Important

If the recording server is formatted, a new counter-password is generated by the server. Thus, a new registration must be made.

4.1 How to configure the licenses

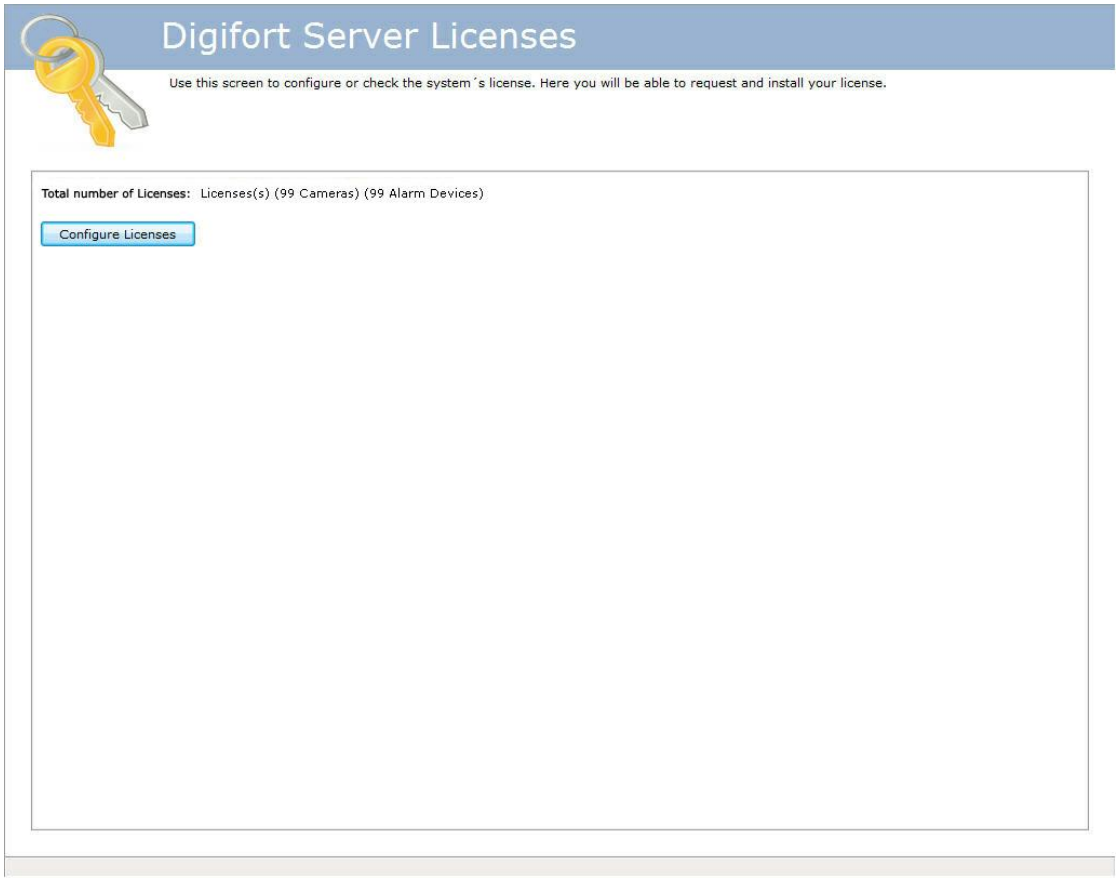
Before starting your server, make sure that the HardKey which is sold together with the software is correctly connected to your machine.

To start the licensing of Digifort, after logging in to the server, find the Licenses item located on the server's Configurations Menu, as shown in the picture below

© 2002 - 2011 by Optiview USA all rights



Once this is done, information about Digifort's present licensing state will appear at the right as shown in the picture below


Digifort Server Licenses
Use this screen to configure or check the system´s license. Here you will be able to request and install your license.
Total number of Licenses: Licenses(s) (99 Cameras) (99 Alarm Devices)
Configure Licenses

We can take the following information from this screen:

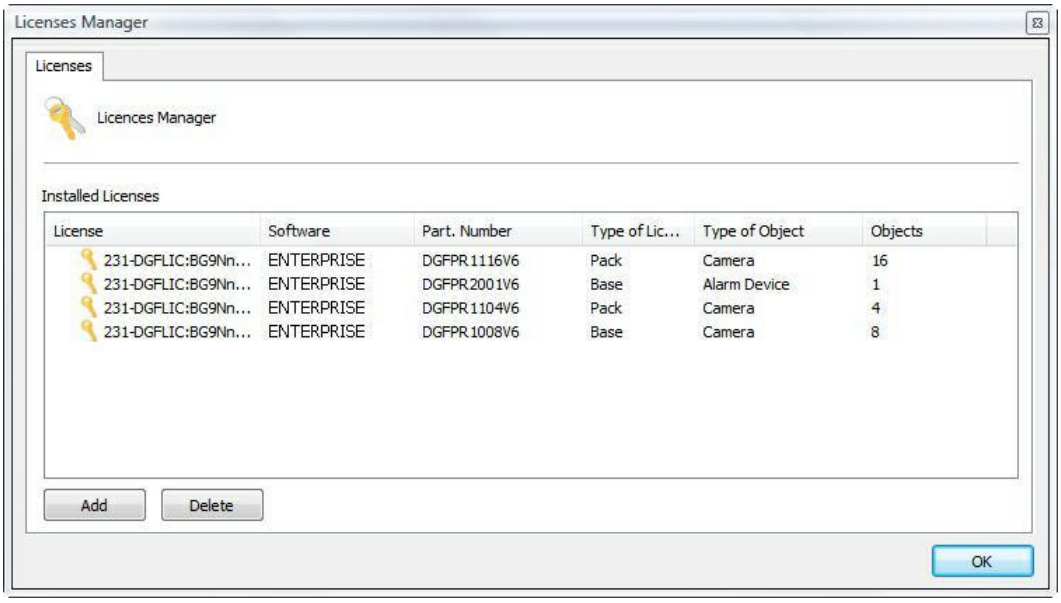
- **Total of licenses**: Number of licenses installed in the server, followed by the number of cameras with recording support, and the number of alarm devices with surveillance

© 2002 - 2011 by Optiview USA all rights

support.

- **Base license**: The name of the company to which this software is licensed appears in this field.

To configure the server's licenses, click on the **Configure Licences** button. This action will result in execution of the Licences Administrator, as shown in the picture below:



In this screen, all of the licenses installed in the server are displayed. To add a license, click on the button **Add** and to remove a license, select the desired license and click on the **Remove** Button.

At the end of the configuration, click on **OK** to close the screen.

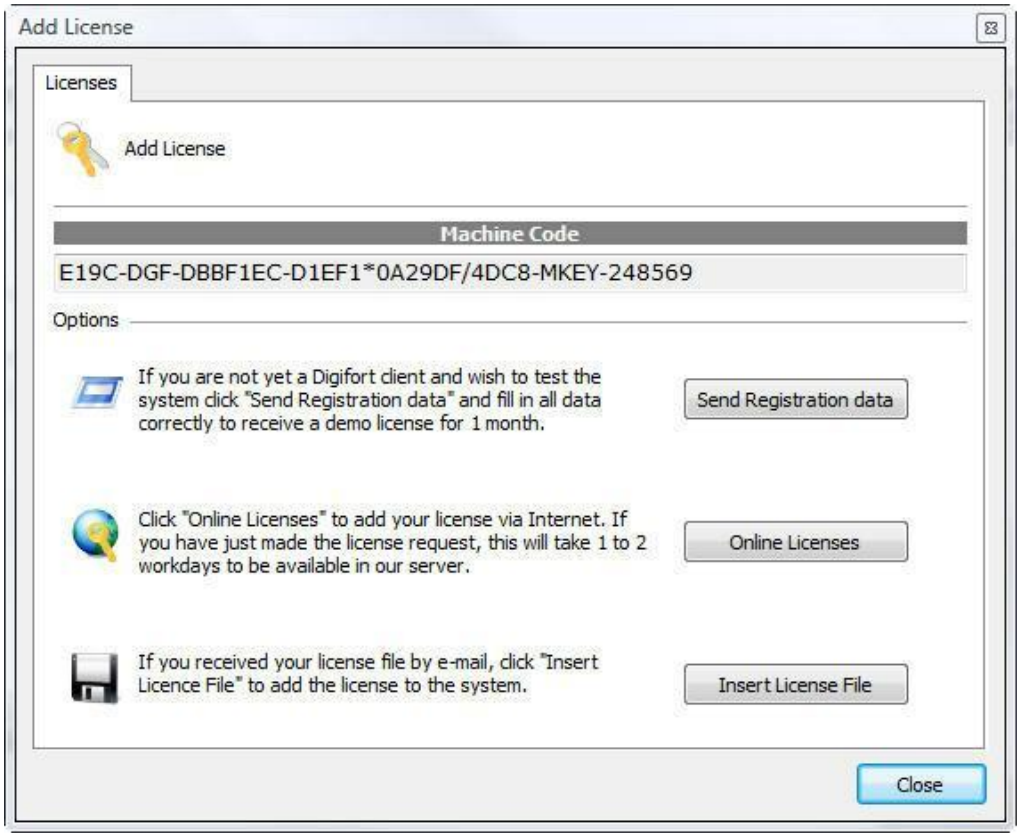
Observation

If the base license is removed, the pack licenses will not be loaded and will disappear automatically from the screen. The pack licenses can only be loaded if the base license is installed.

4.1.1 How to add a license

To add a license, click on the **Add** button in the License Administrator. The screen for adding licenses will be displayed as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights


Add License
Licenses
Add License
Machine Code
E19C-DGF-DBBF1EC-D1EF1*0A29DF/4DC8-MKEY-248569
Options
If you are not yet a Digifort client and wish to test the system click "Send Registration data" and fill in all data correctly to receive a demo license for 1 month.
Send Registration data
Click "Online Licenses" to add your license via Internet. If you have just made the license request, this will take 1 to 2 workdays to be available in our server.
Online Licenses
If you received your license file by e-mail, click "Insert Licence File" to add the license to the system.
Insert License File
Close

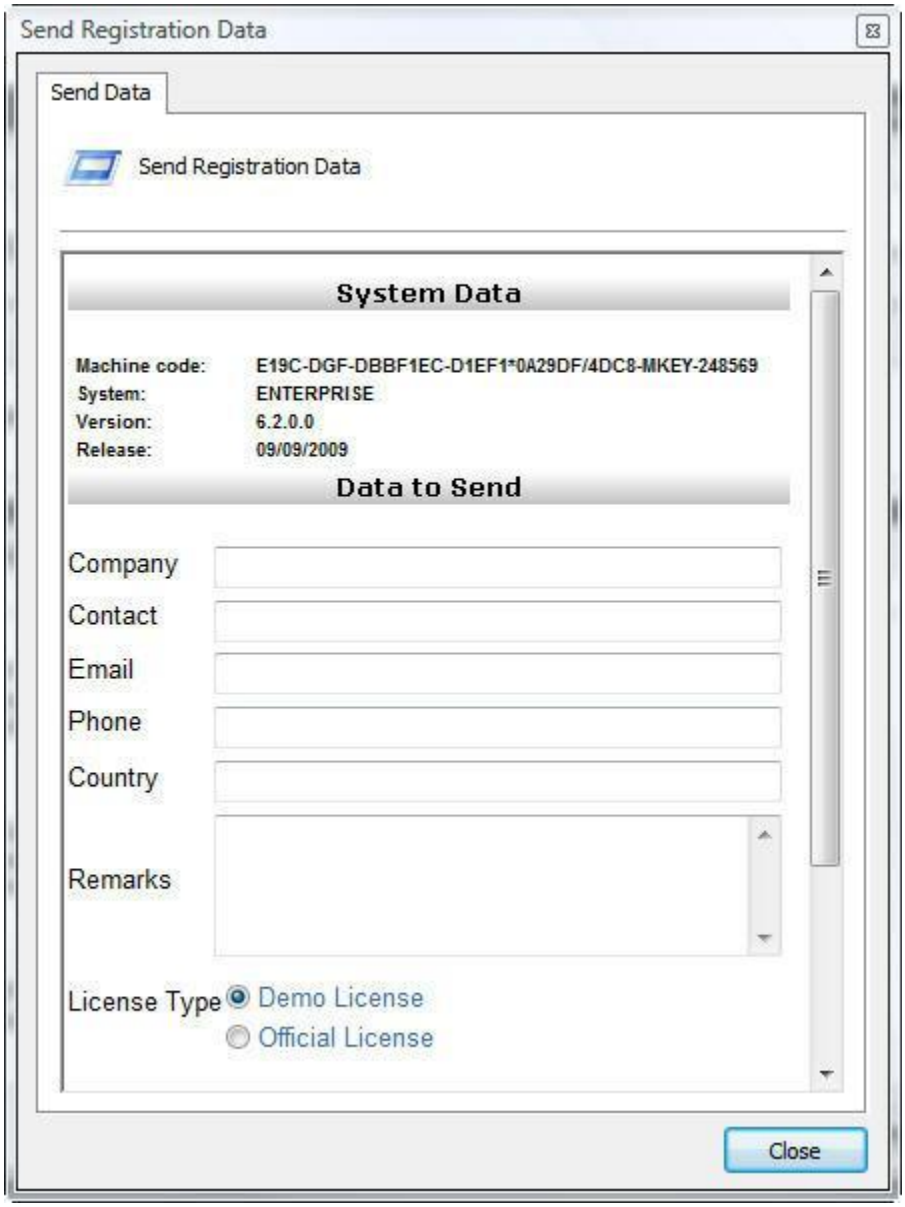
4.1.2 How to send data for registration

The first phase in licensing Digifort is the sending of data for registration. This process consists of filling out the user's data which will be sent together with the counter password of the server to the Licensing Center.

With this data at hand, the Licensing Center will generate the requested licenses and a confirmation will be sent to the supplied e-mail address.

To start the process of sending registration data, click on **Send data for Registration**. This action will open a form to be filled out with the client's data, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



After correctly filling in the fields, click on the **Send** button. Your license will be generated in at most two weekdays. When your license is finished, you will receive a confirmation letter by e-mail with all of the instructions for installing the license.

These instructions are also described in the following pages of this manual.

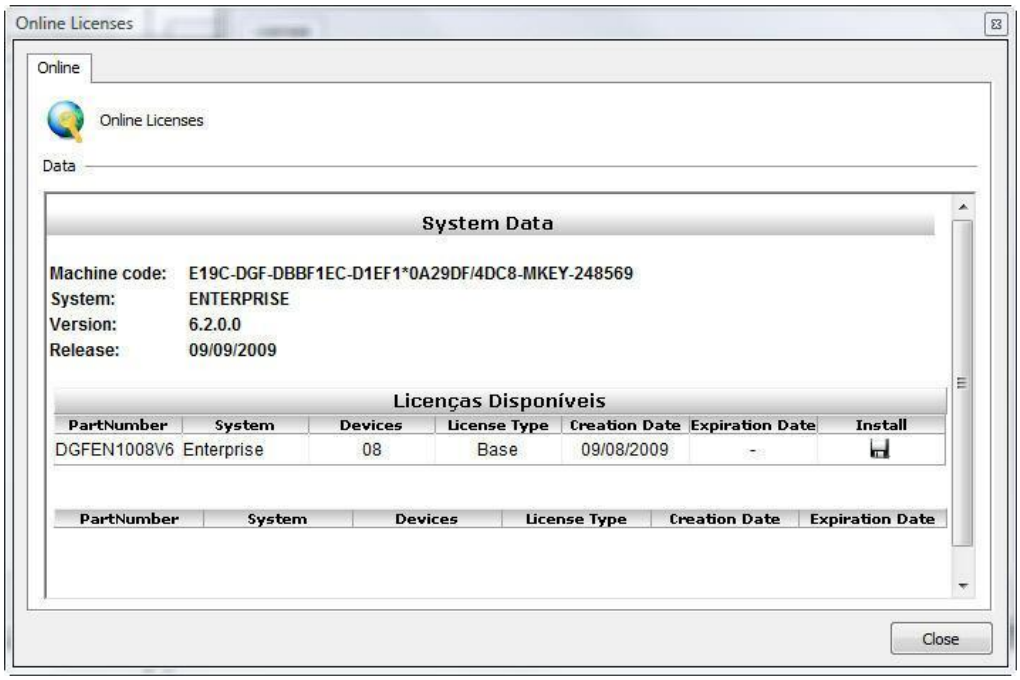
4.1.3 How to install licenses via Online Licenses

Licensing via Online Licenses is the safest and most practical way to license Digifort.

After receiving the license confirmation e-mail, click on the **Online Licenses**

© 2002 - 2011 by Optiview USA all rights

button. A window will be opened listing all of the available licenses for your server, as shown in the picture below:



To install the licences, locate the desired license and then click on the icon in the Install column. In the case of installation of official licenses, install the base license first, then all of the pack licenses. And in the case of demonstration license installation, install it normally.

After installation of the licenses, click on the **Close** button.

4.1.4 How to install licenses via license files

In case your server has no access to Internet, you must use licensing via license files. To carry out this process, copy the counter password of your server and send it via e-mail to Digifort. Your license will be generated using this counter password. Soon afterwards, the license files will be sent to your e-mail address.

To install the license files in the Digifort Server, copy them to the server or to some network unit that it has access to and click on Insert License File. A window should open requesting the location of the license files.
Locate the files and open first the base license file and afterwards all of the pack license files.

Observation

Some errors can occur using this licensing method. This is due to the fact that the licensing process is being carried out by means outside of the realm of Digifort. The most common errors are: sending of an incorrect counter password and corruption of the license files sent by e-mail. For this reason, try to use the Online Licensing

© 2002 - 2011 by Optiview USA all rights

Observation

method.

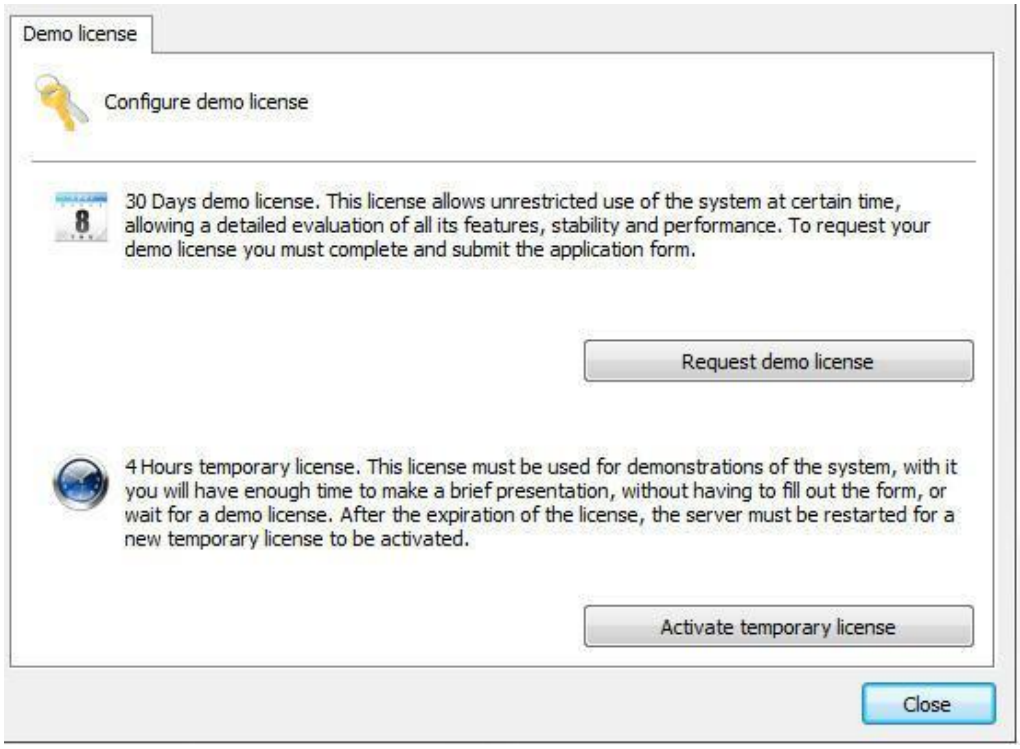
4.1.5 Enabling a temporary license

The temporary license feature was created to enable the software demo. Once the temporary license is activated, the software will work for two hours.

To activate the temporary license click on the Demo License button as shown in the Picture below:

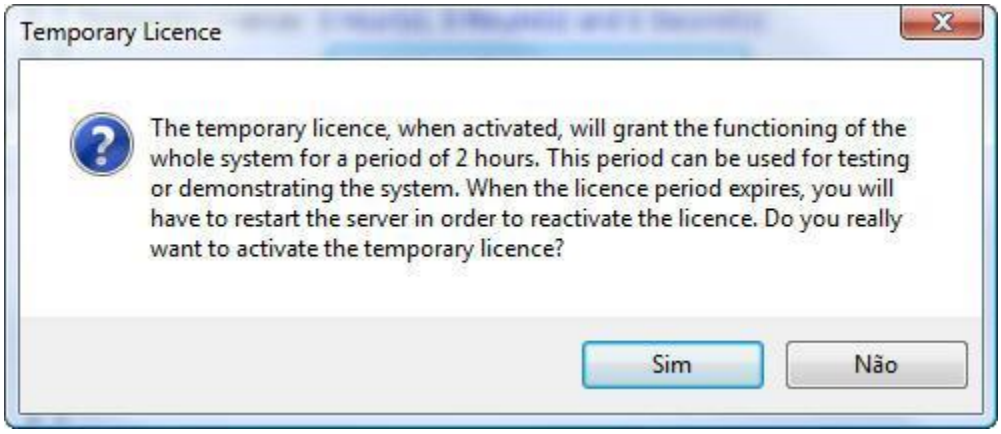

Total number of Licenses: 0 License(s) (0 Cameras) (0 Alarm Devices)
Temporary License: 0 Hour(s), 0 Minute(s) and 0 Second(s)
Configure Licenses
Demo license

Then click on Activate temporary license as shown in the picture below:


Demo license
Configure demo license
30 Days demo license. This license allows unrestricted use of the system at certain time, allowing a detailed evaluation of all its features, stability and performance. To request your demo license you must complete and submit the application form.
Request demo license
4 Hours temporary license. This license must be used for demonstrations of the system, with it you will have enough time to make a brief presentation, without having to fill out the form, or wait for a demo license. After the expiration of the license, the server must be restarted for a new temporary license to be activated.
Activate temporary license
Close

You will see the window shown below; click on yes to install the license.

© 2002 - 2011 by Optiview USA all rights


Temporary Licence
The temporary licence, when activated, will grant the functioning of the whole system for a period of 2 hours. This period can be used for testing or demonstrating the system. When the licence period expires, you will have to restart the server in order to reactivate the licence. Do you really want to activate the temporary licence?
Sim
Não

© 2002 - 2011 by Optiview USA all rights

Chapter V

5 Registering Digifort

After licensing Digifort, it is necessary to register it. The registration of Digifort will guarantee that you receive notifications of product updates, news and special offers. It will also guarantee that you receive technical support and installation support, as well as additional benefits.

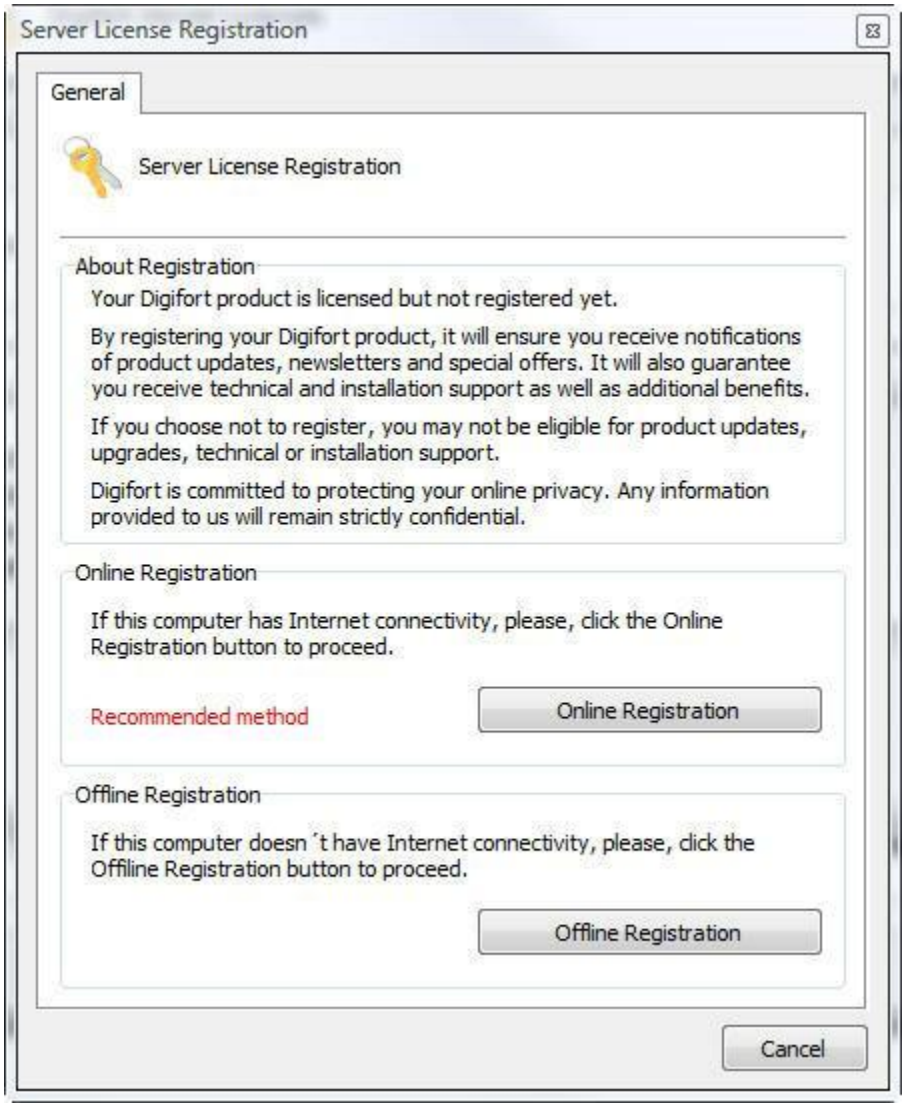
If you decide not to register, you will not be eligible for updates, upgrades, technical support or installation support.

Registering Digifort, you will receive a registration code which, for security reasons, will also be stored in our licensing center. If you use a hard key and it becomes necessary to format the Server or reinstall Digifort, out licensing Center will identify your server and will automatically register it again.

5.1 How to register Digifort

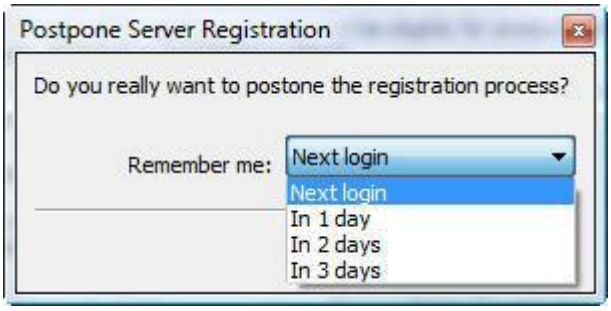
After inserting your usage license, the software's registration window will automatically be displayed, as shown in the figure below. To understand how to install licenses in Digifort, see Licensing Digifort.

© 2002 - 2011 by Optiview USA all rights


Server License Registration
General
Server License Registration
About Registration
Your Digifort product is licensed but not registered yet.
By registering your Digifort product, it will ensure you receive notifications of product updates, newsletters and special offers. It will also guarantee you receive technical and installation support as well as additional benefits.
If you choose not to register, you may not be eligible for product updates, upgrades, technical or installation support.
Digifort is committed to protecting your online privacy. Any information provided to us will remain strictly confidential.
Online Registration
If this computer has Internet connectivity, please, click the Online Registration button to proceed.
Recommended method
Online Registration
Offline Registration
If this computer doesn´t have Internet connectivity, please, click the Offline Registration button to proceed.
Offline Registration
Cancel

Registration of Digifort can be done in two ways, Online and Offline. The Online method is recommended, but can be used only when the computer which is executing the Administration Client is connected to Internet. The Offline method must be used when the computer has no access to Internet.

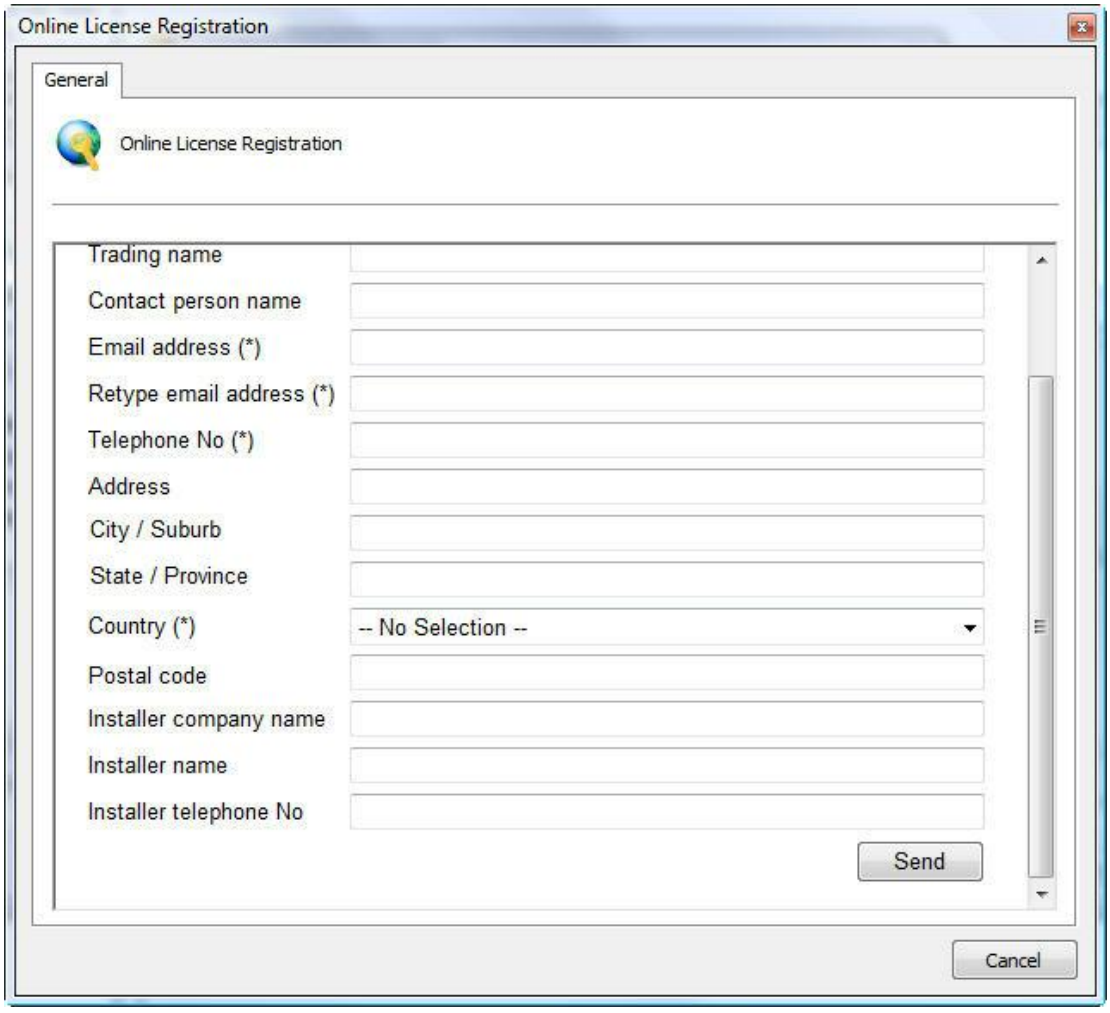
If you wish to register later, close this window and select the desired option, as shown below:



© 2002 - 2011 by Optiview USA all rights

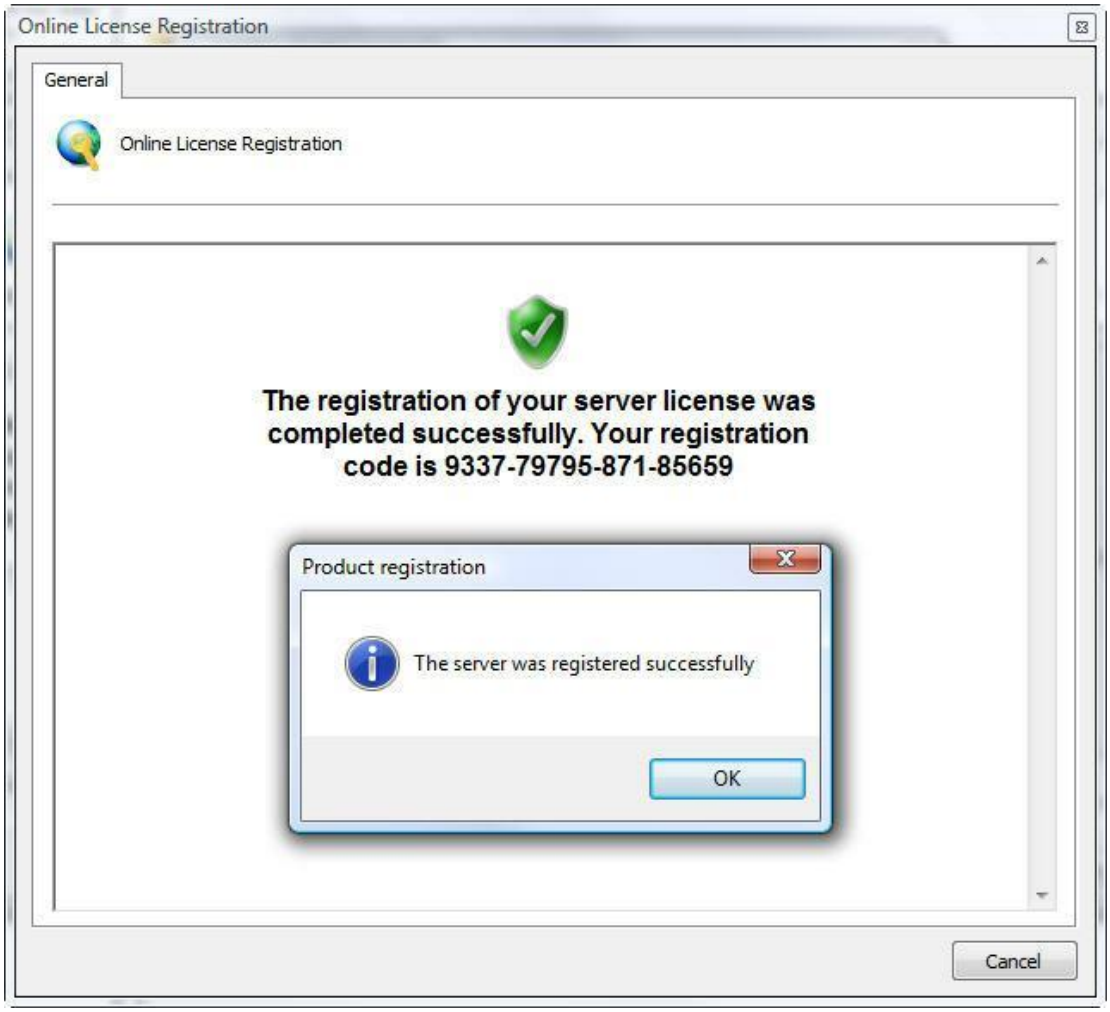
5.2 Registering Digifort Online

To register Digifort online, click on the Register Online Button. A screen will be displayed with the form to be filled out, as shown in the figure below:



Fill in all of the fields and click on Send. A registration confirmation screen will be displayed, together with your registration code, as shown in the figure below

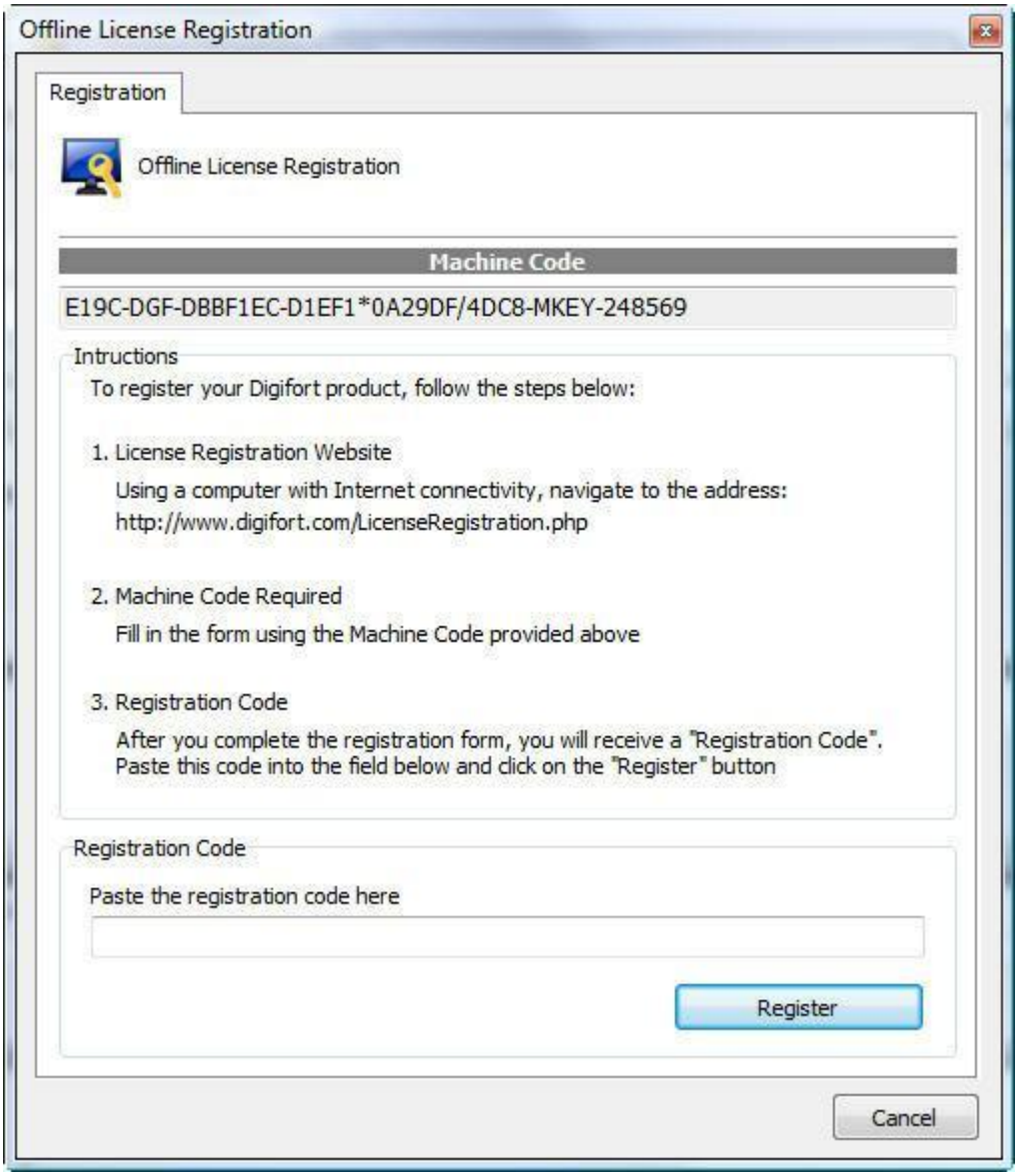
© 2002 - 2011 by Optiview USA all rights



5.3 Registering Digifort Offline

To register Digifort offline, click on the **Register Offline** button. A screen will be displayed with instructions on how to register Digifort. Follow the instructions shown in the screen and click on **Register**.

© 2002 - 2011 by Optiview USA all rights


Offline License Registration
Registration
Offline License Registration
Machine Code
E19C-DGF-DBBF1EC-D1EF1*0A29DF/4DC8-MKEY-248569
Intructions
To register your Digifort product, follow the steps below:
1. License Registration Website
Using a computer with Internet connectivity, navigate to the address:
http://www.digifort.com/LicenseRegistration.php
2. Machine Code Required
Fill in the form using the Machine Code provided above
3. Registration Code
After you complete the registration form, you will receive a "Registration Code".
Paste this code into the field below and click on the "Register" button
Registration Code
Paste the registration code here
Register
Cancel

© 2002 - 2011 by Optiview USA all rights

Chapter VI

6 Recording Server

This chapter is dedicated to the Recording Server of the Digifort System. It is in this module that the cameras are registered and their functioning is monitored.

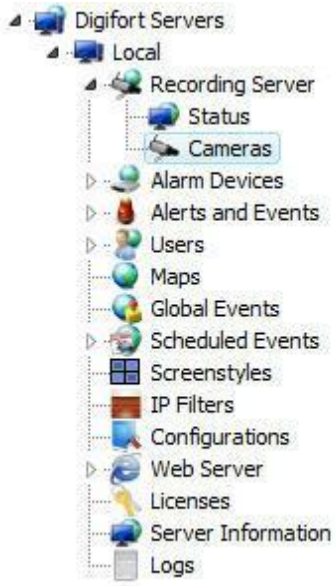
The Recording Server is divided into two modules, the Camera module where the cameras are registered, and the Status module where the functioning of the cameras is monitored.

The Digifort System works with the main brands of digital cameras in the market and accepts analogical cameras as long as they are connected by way of a video-server device. These cameras can be located at the same site where the server is or can be remotely connected by way of some network connection. The main attributes of the configuration of the cameras, such as image resolution, number of frames per second and visualization rights are configured in the Digifort System and automatically applied to the cameras, regardless of location and without stopping the recording of the other cameras.

The Register of Cameras is one of the most critical parts of the system, since a bad configuration can lead to the malfunctioning of the system. Therefore, careful planning must be done beforehand, collecting data such as the number of cameras, desired number of frames per second, days of storage, available disk space, etc.

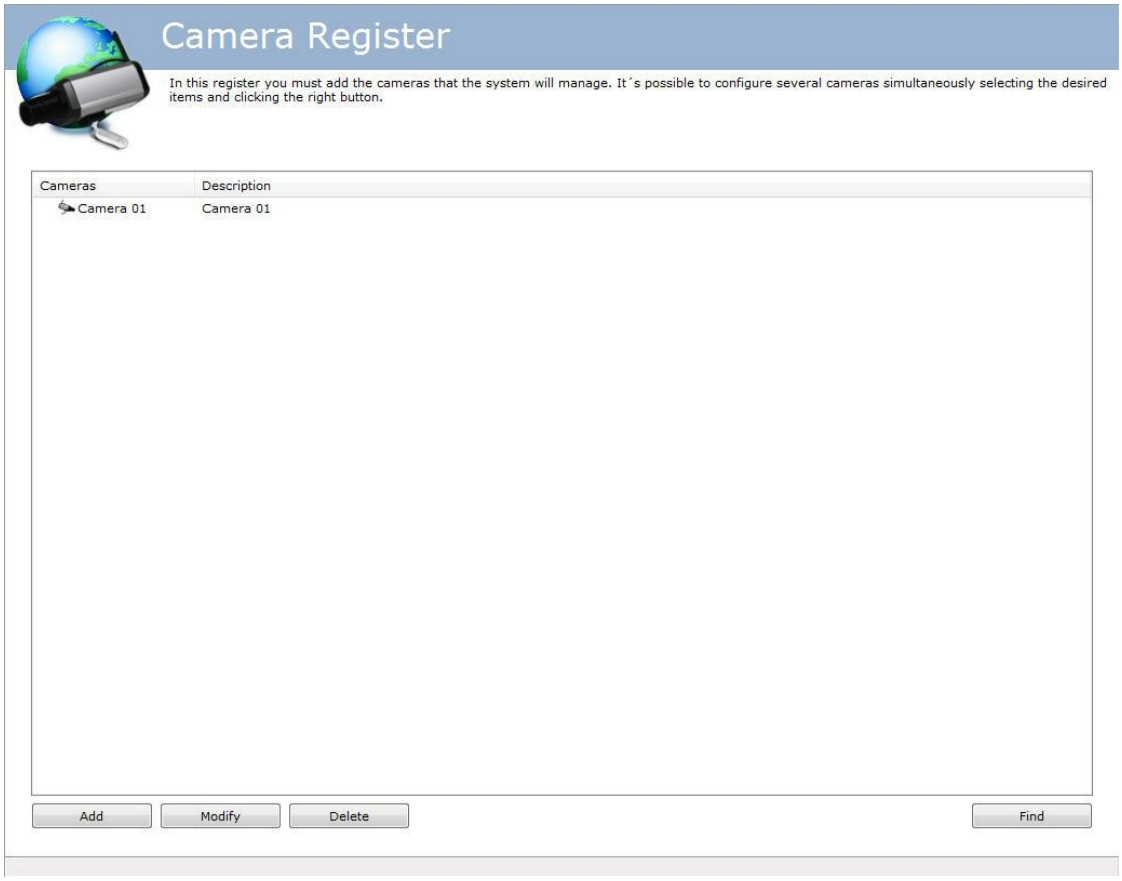
6.1 How to add a camera

To access the Register of Cameras, locate the Recording Server icon and then click on the Cameras icon, as shown in the picture below:



Once this is done the register of cameras will be executed, as shown in the picture below:

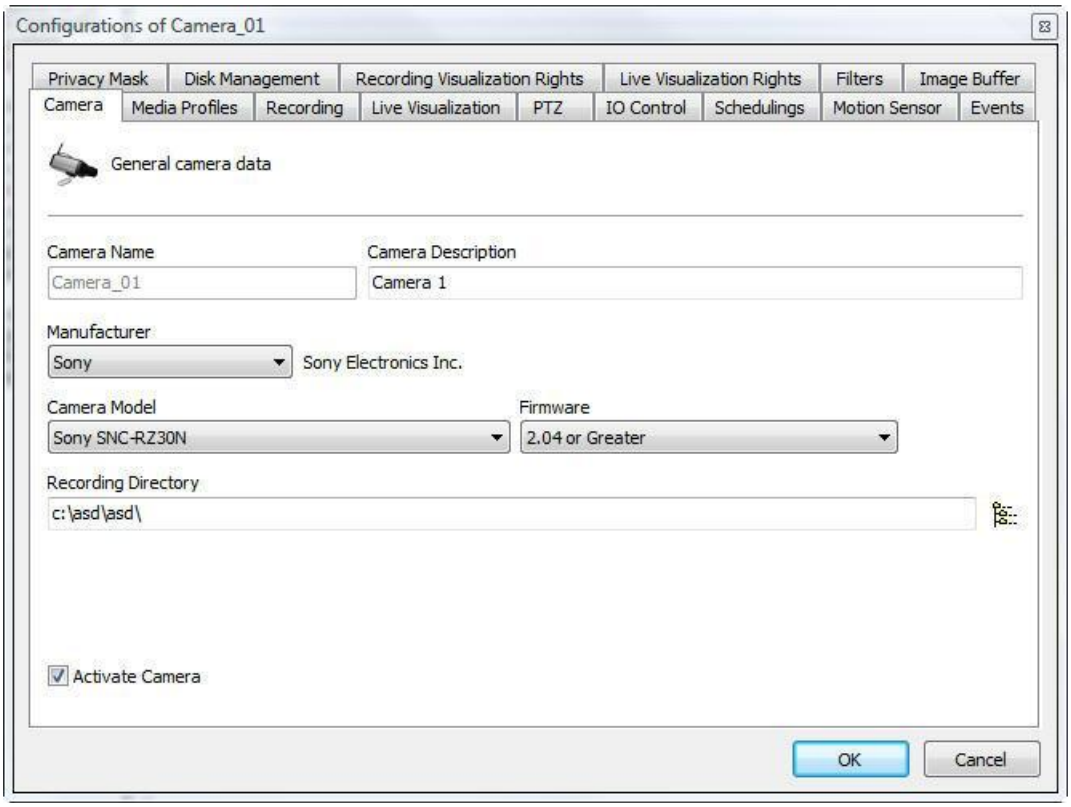
© 2002 - 2011 by Optiview USA all rights


Camera Register
In this register you must add the cameras that the system will manage. It´s possible to configure several cameras simultaneously selecting the desired items and clicking the right button.
Cameras
Description
Camera 01
Camera 01
Add
Modify
Delete
Find

To add a camera, click on **Add**. To modify or remove a camera, select the desired camera and click on the corresponding button.

© 2002 - 2011 by Optiview USA all rights

6.1.1 Camera data



- **Camera Name**: Enter a name for the camera. This name will be used as an internal reference of the system. Therefore, once saved it cannot be modified.

- **Description of the camera**: Enter a short description for the camera to aid in its identification. In the Surveillance Client it is this description that will help to identify each camera.

- **Manufacturer:** Select the manufacturer of the camera to be inserted..

- **Model of the camera:** Select the model of the camera to be inserted.

- **Firmware**: Select the version of the firmware of the camera to be inserted. As default, upon selecting the model of the camera, the last version of the firmware is automatically selected. In most cases, the choice of the most recent firmware allows the camera to work perfectly in all of its modes.

- **Video port**: If the device to be inserted it a video-server, select the number of the port on which the camera is found. This field will only visible for video-servers with more than one port.

- **Recording directory** Digifort allows camera recording to be distributed among several disks. For this purpose, select the recording directory for images of the camera to be inserted. It's possible to record in network units, that is, in the disks of

© 2002 - 2011 by Optiview USA all rights

other computers in the network. To learn how to use this feature, see Network Units.

- **Activate camera**: Indicates whether the system must record the images received from the camera.

Attention

Digifort is responsible for administrating the structure of directories used in camera recording. Therefore, no file of its database should be excluded manually, and the camera recording directory may not be created by any means other than Digifort such as, for example, Windows Explorer.

6.1.2 Media profiles

A media profile consists of a set or individual parameters of each camera such as image resolution, frames per second and image quality, that are associated with Recording and Live Visualization.
For better understanding, let's take the following situation: A recording profile could be created, that will be associated to the camera recording event. In this profile we could define that we want to record five frames per second, with a resolution of 320x240 and with high image compression. A visualization profile could also be created, that will be associated to visualization of the camera. In this profile we could define that we want to visualize the camera at ten frames per second with a resolution of 640x480 and low image compression.

As default, upon registering a new camera, two pre-defined media profiles are created, one for recording and one for visualization. The pre-configured parameters of each profile are only those parameters in common to all devices. The Media Profiles of most cameras and video-servers have parameters in common and individual parameters of each piece of equipment. The common parameters are:

- **Video compression**: The video compression to be used in recording images in disk. At present, Digifort supports the Motion JPEG and Wavelet formats..

- **Image resolution**: The image resolution that will be used in the profile. Upon selecting the model of the camera, this resolution list will automatically display only the resolutions supported by that camera. A very high image resolution will use up much disk space and bandwidth in your network, but the image will have a superior quality in which we will be able to recognize more detail in the image, such as, for example, the face of a person. A very low image resolution will use up little disk space and bandwidth in your network, but the image will have an inferior quality, giving few details. This parameter should be well configured according to your needs. Digifort has a calculator for disk space use that will help you to better configure the image resolution and frames per second. To learn how to use the Digifort calculator, see Calculator for disk space usage.

- **Image quality**: The images coming from the cameras go through a compression process. The higher the image compression level, the less quality the image will have, and the lower the image compression level, the more quality the image will have. Digifort offers five quality levels ranging from High (low compression) and

© 2002 - 2011 by Optiview USA all rights

Low (high compression). After various laboratory tests we recommend the Medium quality, as it offers an excellent image quality and low network traffic and low disk space usage.

- **Frames per second**: The number of frames per second to be recorded. A greater frames-per-second rate will use up more bandwidth in your network and more disk space, but will offer smoother movement. A lower rate of frames per second will use up less bandwidth in your network and less disk space, but the movement will be jerkier. It has been scientifically proven that at three to seven frames per second, it is possible to recognize all movements of a person. In some cases, it might not be possible for the camera to send the configured number of frames per second, especially at high frames-per-second rates. This is due to various factors, such as the bad functioning of the internal network, the number of connections made to the camera and the processing power of the camera.

As parameters specific to an individual piece of equipment, we can cite insertion of text into the image, image rotation, color levels, etc.

Some cameras may not support the adjustment of common parameters, such as, for example, the frame rate and the image quality. In these cases, adjustments must be made directly in the camera using its own interface.

6.1.2.1 How the Media Profiles save network bandwidth

The media profiles also help to save network bandwidth. To explain this concept, first we will define two media profiles, described below:

"Recording" Media Profile	
Parameter	**Value**
Video compression	Motion JPEG
Image resolution	640x480
Image quality	Medium
Frame rate	4 fps

"Visualization" Media Profile	
Parameter	**Value**
Video compression	Motion JPEG
Image resolution	640x480
Image quality	Média
Frame rate	30 fps

Obs: Digifort operates with any resolution supplied by the camera, whether it is low or high resolution (HD) and with any commercially available compression formats (Motion JPEG, MPEG4 and H264).

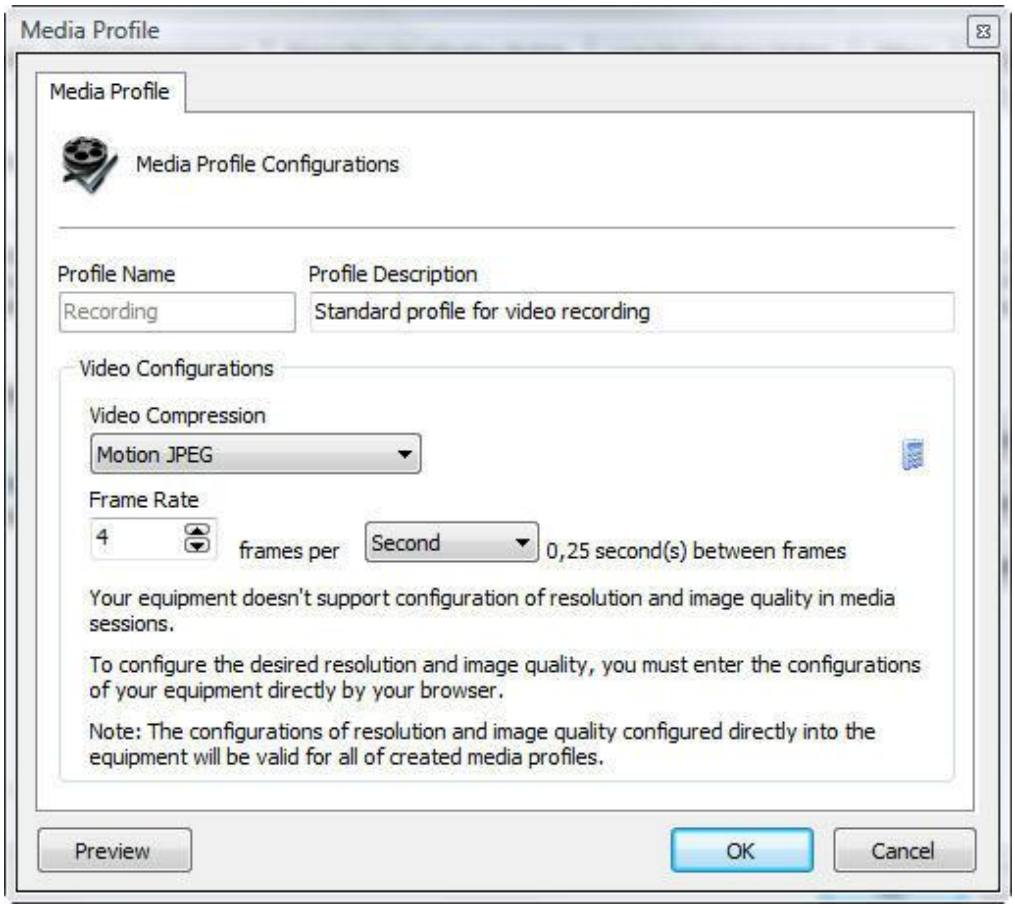
As we can see in the two examples of Media Profiles, all of the parameters of the "Recording" profile are the same as those of the "Visualization" profile, except the Frame rate. With this type of configuration, where only the frame rate is different, Digifort save bandwidth in this way: Let's suppose that the server is recording the images generated normally by the
camera with the associated "Recording" profile. In this case, it will be receiving only four frames per second. In a certain moment, the user wants to visualize this same camera in the Surveillance Client at a frame rate of 30 frames per second. At this moment, Digifort recognizes that the configurations are the same, with only the

© 2002 - 2011 by Optiview USA all rights

visualization frame rate being higher than the recording frame rate. Instead of the server making a new connection to the camera to receive the desired 30 frames per second, it closes the present connection and opens a new connection receiving the 30 frames per second, applying a frames speed filter on the recording profile, limiting its velocity to 4 frames per second. This way, only one connection is maintained with the camera receiving only 30 frames per second instead of two connections receiving a total of 34 frames per second.

6.1.2.1.1 How to add Media Profiles

To add a media profile, click on **Add**, and the media profile adding screen will be displayed as shown in the picture below:


Media Profile
Media Profile
Media Profile Configurations
Profile Name
Recording
Profile Description
Standard profile for video recording
Video Configurations
Video Compression
Motion JPEG
Frame Rate
4
frames per
Second
0,25 second(s) between frames
Your equipment doesn't support configuration of resolution and image quality in media sessions.
To configure the desired resolution and image quality, you must enter the configurations of your equipment directly by your browser.
Note: The configurations of resolution and image quality configured directly into the equipment will be valid for all of created media profiles.
Preview
OK
Cancel

It's important to point out that this screen can vary from camera to camera, since each one has its own set of configuration parameters.

In the example above, the selected camera doesn't support adjustment of image resolution and quality.

© 2002 - 2011 by Optiview USA all rights

6.1.2.1.2 How to visualize the functioning of the configured media profile

To visualize the results of the configurations of the parameters of the media profile being edited, click on the Preview button, opening a screen with the live image of the camera, as shown in the picture below:

This function will only work if the camera's connection address was previously informed. To learn now to configure this parameter, see How to configure the recording of the camera.



In this screen, the following configurations are informed:

- **Received frames per second:** Informs the number of frames per second received.
- **Image size**: Informs the size of the received image in KB/s and in Kbps. These values help in the dimensioning of the disk space and network bandwidth that this camera occupies..
- **Decoder codec**: The codec used for decoding the image. Digifort uses various decoding codecs. When the camera is added, the codec that has the best performance based on the received image is automatically identified.

Observation

All information contained in the image is updated every second.

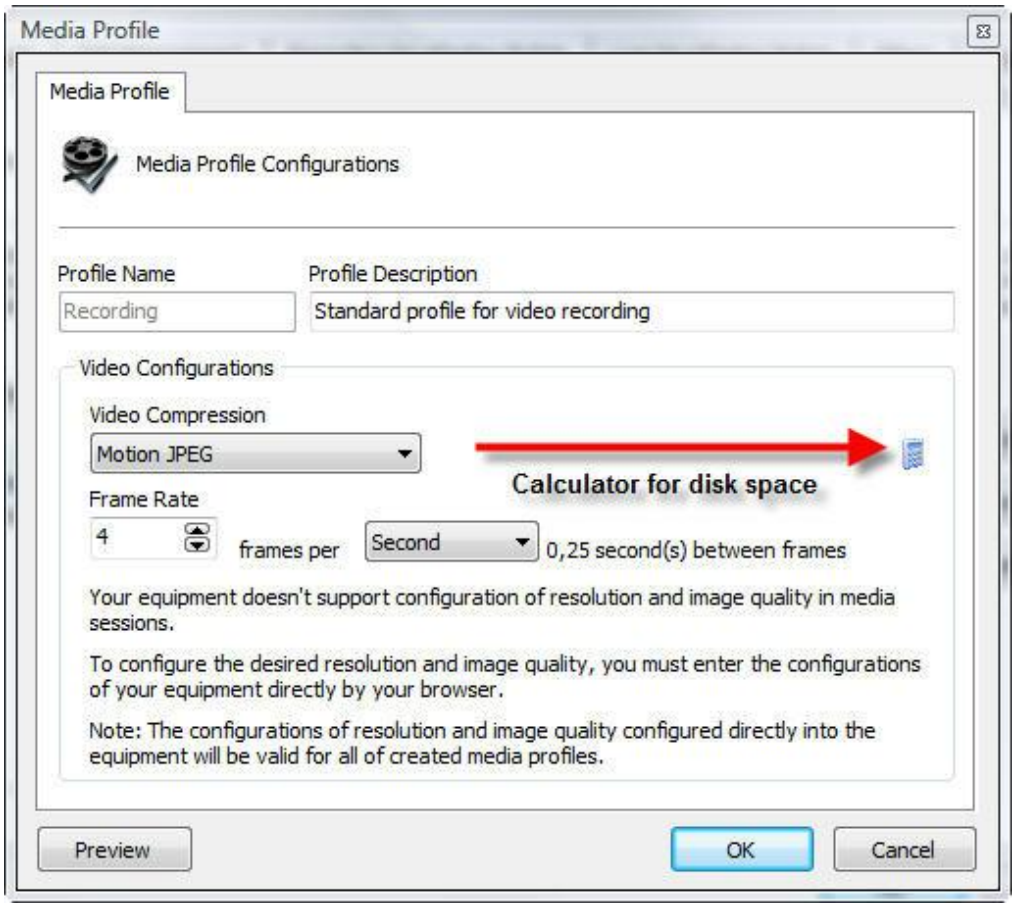
6.1.2.1.3 Calculator for disk space usage

Digifort has a very useful tool to aid in the dimensioning of disk space to be reserved for

© 2002 - 2011 by Optiview USA all rights

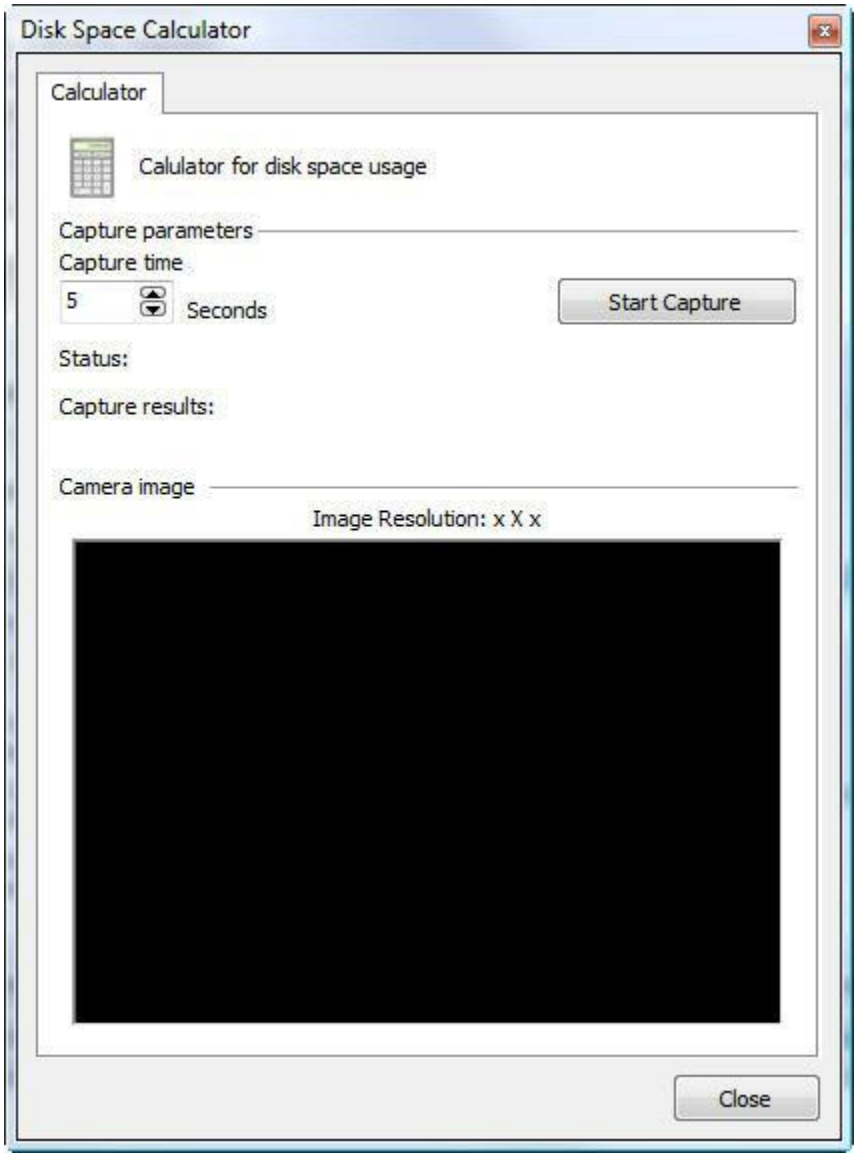
each camera: the disk space usage calculator. To access this feature, click on the button identified by a “calculator”, on the media profile configuration screen, as shown in the picture below:

This function will only work if the camera’s connection address was previously informed. To learn how to configure this parameter, see How to configure the recording of the camera.


Media Profile
Media Profile
Media Profile Configurations
Profile Name
Recording
Profile Description
Standard profile for video recording
Video Configurations
Video Compression
Motion JPEG
Calculator for disk space
Frame Rate
4
frames per
Second
0,25 second(s) between frames
Your equipment doesn't support configuration of resolution and image quality in media sessions.
To configure the desired resolution and image quality, you must enter the configurations of your equipment directly by your browser.
Note: The configurations of resolution and image quality configured directly into the equipment will be valid for all of created media profiles.
Preview
OK
Cancel

Clicking on this button, the disk space calculator will be executed as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights

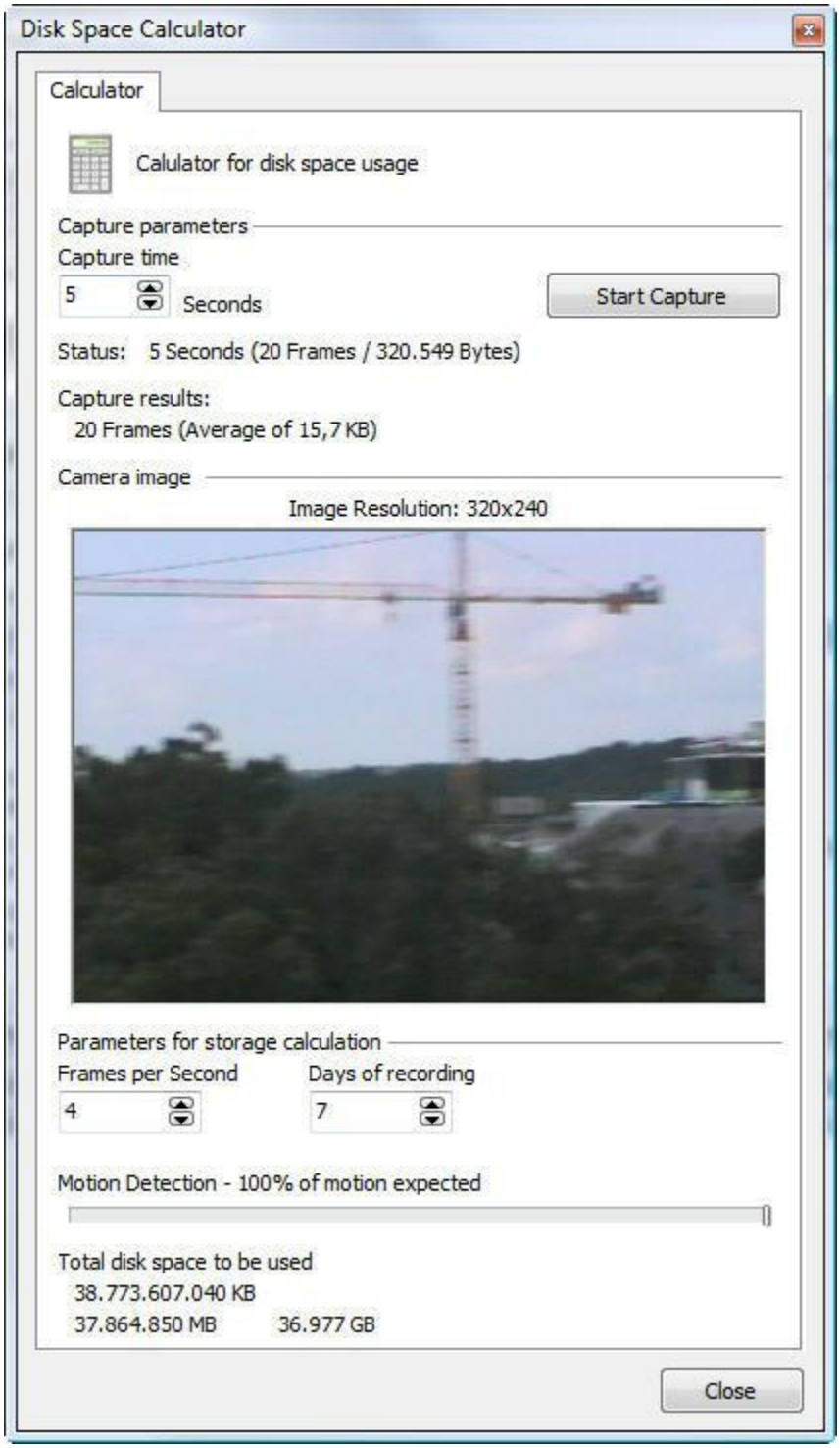


To calculate the disk space necessary for the recording of the camera, the calculator captures an original temporary video from the camera with the parameters of image quality and resolution configured in the media profile being edited and the capture time informed in this screen. Based on the video received, a calculation in made to determine the size of the disk space necessary for storing the images generated by this camera a given number of days and the expected motion detection rate.

To start the process of disk space calculation, inform the capture time value and then click on Start Capture.

Once this is done, the video is captured and analyzed, displaying the screen below:

© 2002 - 2011 by Optiview USA all rights



After the end of the analysis of the captured video, the calculator fills the maximum frames-per-second value that the camera is able to send, that is, if the media profile was configured for recording at 30 frames per second, but the camera is only able to send 12 frames, this value will be 12. Modify the values of frames per second, days of recording and estimation of the motion detection to get an estimation of the

© 2002 - 2011 by Optiview USA all rights

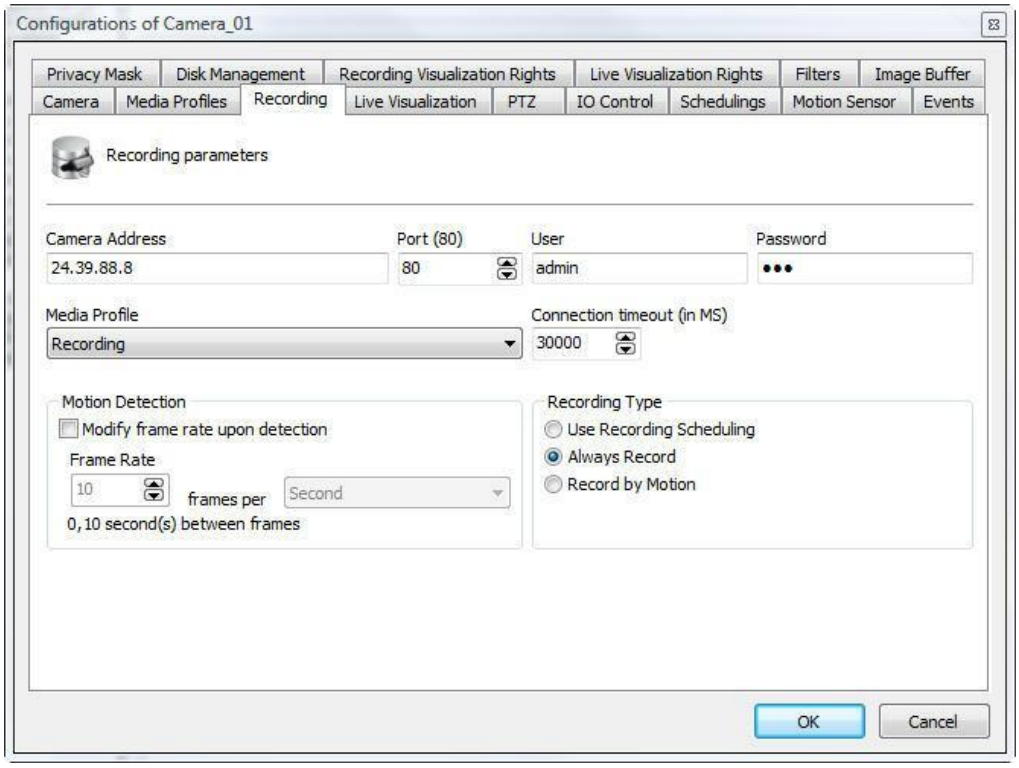
occupation of disk space to be used by the camera. Below are descriptions of how each parameter of the space calculator works.

- **Days of recording:** Informs the number of days to be stored for this camera. The greater this value is, the more disk space is used.
- **Frames per second:** Informs the number of frames per second to be used in recording of the camera.
- **Motion detection:** Informs the percentage of motion expected at the location of the camera in a day. For example, if the normal operation of a camera doesn't detect motion at night, then we slide this control, adjusting its value to 50%.
- **Total of disk to be used:** Informs the disk space necessary for storing the images generated by the camera with the parameters configured in the media profile being edited, the number of storage days and the percentage of motion configured.
- **Calculate size:** Click on this button to recalculate the disk space necessary for storage of the images of this camera with a new image.

6.1.3 How to configure the recording of the camera

After registering the media profiles to be used, it's necessary to associate them to the recordings and visualization events of the camera.

To access this configuration, click on the Recording tab, as shown in the picture below:



© 2002 - 2011 by Optiview USA all rights

6.1.3.1 Camera address

IP or DNS address of the camera. The IP address to be used must already be internally configured in the camera.

6.1.3.2 Port

The port for communication with the camera. Most cameras in the market use port 80 for connection. The port to be used must already be internally configured in the camera.

6.1.3.3 User and Password

Informs the user who Digifort will use to carry out the authentication of the camera. Consult the manual of your camera to find the standard user and how to add more users.

Informs the password that Digifort will use to carry out the authentication of the camera. Consult the manual of your camera to find the standard password and how to modify it.

Important: it's recommended that you inform the user and the password of the camera in the correct fields, as some camera features depend on this information for previous authentication and execution of the requested command. The user to be supplied must be the administrator user of the camera. To get this information, consult the user manual of your camera.

6.1.3.4 Connection timeout (in MS)

This parameter is used by the system when the connection with the camera is somehow lost. Then, every X milliseconds the system will try to re-establish the connection, where X is the specified value. To convert this value to seconds, simply divide this value by 1,000. By default, this parameter is already configured at 4000ms (4 seconds).

6.1.3.5 Type of recording

Digifort Enterprise offers three types of recording: continuous recording (always record), recording by motion detection, and recording by scheduling. Continuous recording will record to disk all images received by the camera. Recording by motion detection will record images only when there is motion. Recording by scheduling permits the configuring of recording times in which the camera will always record, record by motion detection, or not record. In most cases, recording by motion detection or event is the most appropriate, as it drastically reduces disk space used. To learn more about recording by motion detection see How to configure the Motion Sensor.

6.1.3.6 Media profile

Select the media profile to be used in recording of the camera.

© 2002 - 2011 by Optiview USA all rights

6.1.3.7 Motion detection

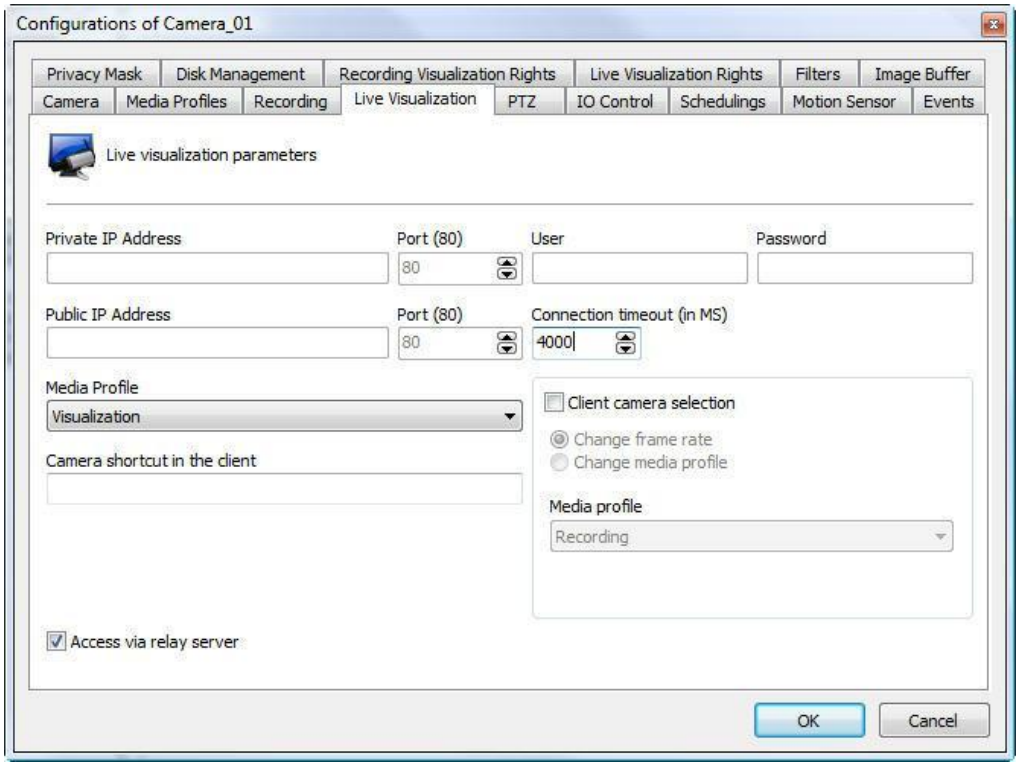
These configurations are applied in the Surveillance Client and work in the following way: when motion is detected in this camera, its frame rate is modified according to the configuration specified here. For example, a camera being monitored at 4 frames per second will have its frame rate modified to 10 frames per second, when motion is detected.

- **Modify the frame rate after detection:** Activates this feature.
- **Frame rate**: Specifies the desired value.

6.1.4 How to configure the visualization of the camera

After registering the media profiles to be used, it's necessary to associate them to the events of recording and visualization of the camera.

To access this configuration, click on the Visualization tab, as shown in the picture below:



The configuration carried out here will be applied to the Surveillance Client, which will use this information to capture the image from the cameras and show on the screen.

The parameters to be configured are described below.

© 2002 - 2011 by Optiview USA all rights

6.1.4.1 This camera will be accessed by the client via relay server

With this option marked, the server will send the client, images that are being recorded in real time using the media profile associated in the Recording tab. With this option marked, no additional configuration is necessary.é necessária.

6.1.4.2 Private IP address

In case access to the camera via relay server is not used, inform the IP address of the camera's local network.

6.1.4.3 Private IP port

Informs the communication port with the camera of your internal network. a porta de comunicação com a câmera de sua rede interna.

6.1.4.4 Public IP address

Digifort also offers the possibility of making a connection with the camera via external network, such as Internet, for example. Fill in the Internet IP address. For this option to work, your router must be configured to supply access to the camera externally.

6.1.4.5 Public IP port

Informs the communication port with the camera via external network. com a câmera através da rede externa.

6.1.4.6 User and Password

User: Informs the user that Digifort will use to carry out authentication on the camera. Consult the manual of your camera to identify the default user and how to add more users.

Password: Informs the password that Digifort will use to carry out authentication on the camera. Consult the manual of your camera to identify the default password and how to modify it.

Important

it's recommended that you inform the user and the password of the camera in the correct fields, as some camera features depend on this information for previous authentication and execution of the requested command. The user to be supplied must be the administrator user of the camera. To get this information, consult the user manual of your camera.

6.1.4.7 Connection timeout (in MS)

This parameter is used by the system when the connection with the camera is

© 2002 - 2011 by Optiview USA all rights

somehow lost. Then, every X milliseconds the system will try to re-establish the connection, where X is the specified value. To convert this value to seconds, simply divide this value by 1000. By default, this parameter is already configured at 4000ms (4 seconds).

6.1.4.8 Media profile

Select the media profile to be used for visualization of the camera. This option will only be available if this camera will be accessed by the client via relay server is unmarked.

6.1.4.9 Short-cut for the camera in the client

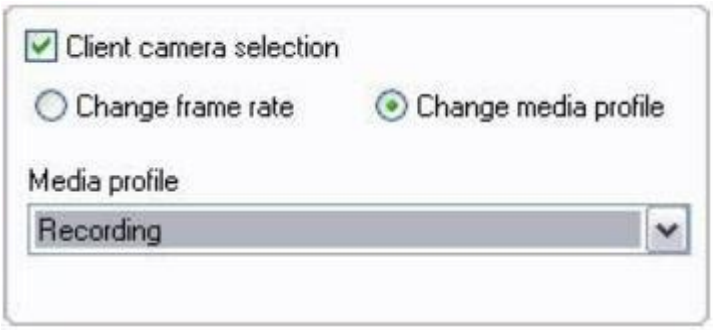
Enter a short-cut name for the camera so that this camera can be rapidly displayed in the Surveillance Client.

6.1.4.10 Selection of camera in the client

Selection of camera in the client: These configurations are applied in the Surveillance Client and work in the following way: when this camera is selected, its frame rate is changed according to the configurations specified here. For example, when a camera being monitored at 4 frames per second is selected, the frame rate is changed to 10 frames per second.

- Modify the frame rate upon detection: Activates this feature.
- Frame rate: Specify the desired value.

Otherwise, you can configure this feature to change the camera media profile, according to the picture below:



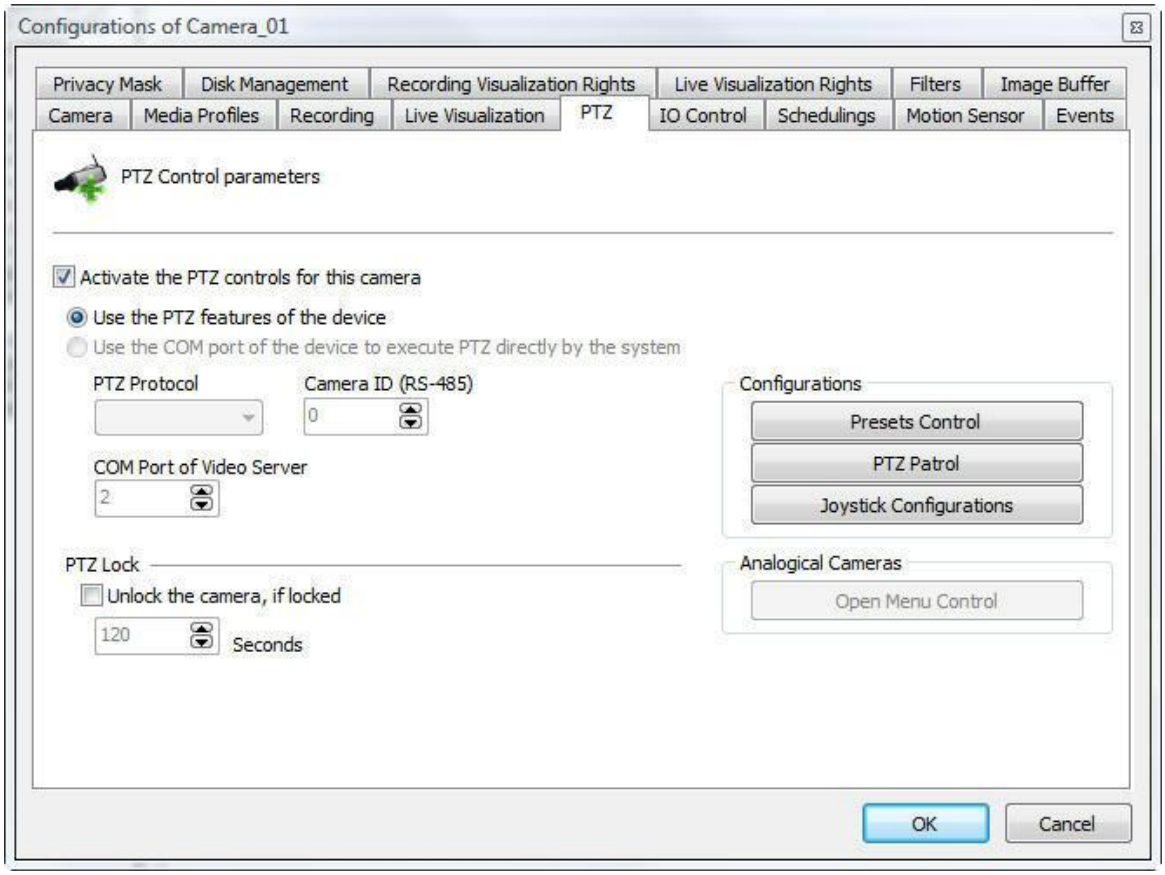
To learn more about Media profile see Media profile

6.1.5 How to configure PTZ

The PTZ configuration allows you to specify the movement parameters of movable cameras.

To access the PTZ configurations, click on the PTZ tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



6.1.5.1 Activate the PTZ control for this camera

Activates the PTZ controls for this camera. If this option in unmarked, movement for this camera will not be available.

6.1.5.2 Use the device's PTZ features

Mark this option only if the camera being registered is an IP camera. In this case, Digifort will send the PTZ commands directly to the camera. para a câmera.

6.1.5.3 Use the device's COM port for the system to carry out PTZ functions directly

Mark this option only if the camera being registered is an analogical camera converted by a video server. In this case, Digifort will send the PTZ commands to the video-server, and then passed on to the camera. para a câmera.

6.1.5.3.1 Select the PTZ protocol

In case the camera being registered is analogical, select the communication protocol that the video server will use for sending the PTZ commands to the

© 2002 - 2011 by Optiview USA all rights

camera.

6.1.5.3.2 Camera ID (RS-485)

In case the camera being registered is analogical, select the camera ID that the video server will use for sending the PTZ commands to the camera.

6.1.5.3.3 COM port of video server

Select the communication port of the video server with the camera. Generally video servers use the COM 2 port.

6.1.5.4 Presets Control button

Opens the presets register, allowing the memorization of camera positions. To learn how to use this feature, see How to configure the Presets Control.

6.1.5.5 PTZ Patrol button

Opens PTZ patrol configuration, allowing you to configure the movement of the camera to certain presets. To learn how to use this feature, see How to configure PTZ Patrol

6.1.5.6 Joystick Configuration button

Opens the joystick configuration, allowing you, among others, to configure the sensitivity and delay of operation. To learn how to use this feature, see How to configure the Joystick

6.1.5.7 Open Menu Controls button

Opens the analog camera configuration screens, allowing the remote configuration of their function such as its ID, for example. To learn how to use this feature, see How to remotely configure analogical cameras

6.1.5.8 How to configure the Presets Control

Presets are memorized positions of a movable camera. With this feature, we can memorize positions, and at any moment rapidly send the focus of the camera to the desired position.

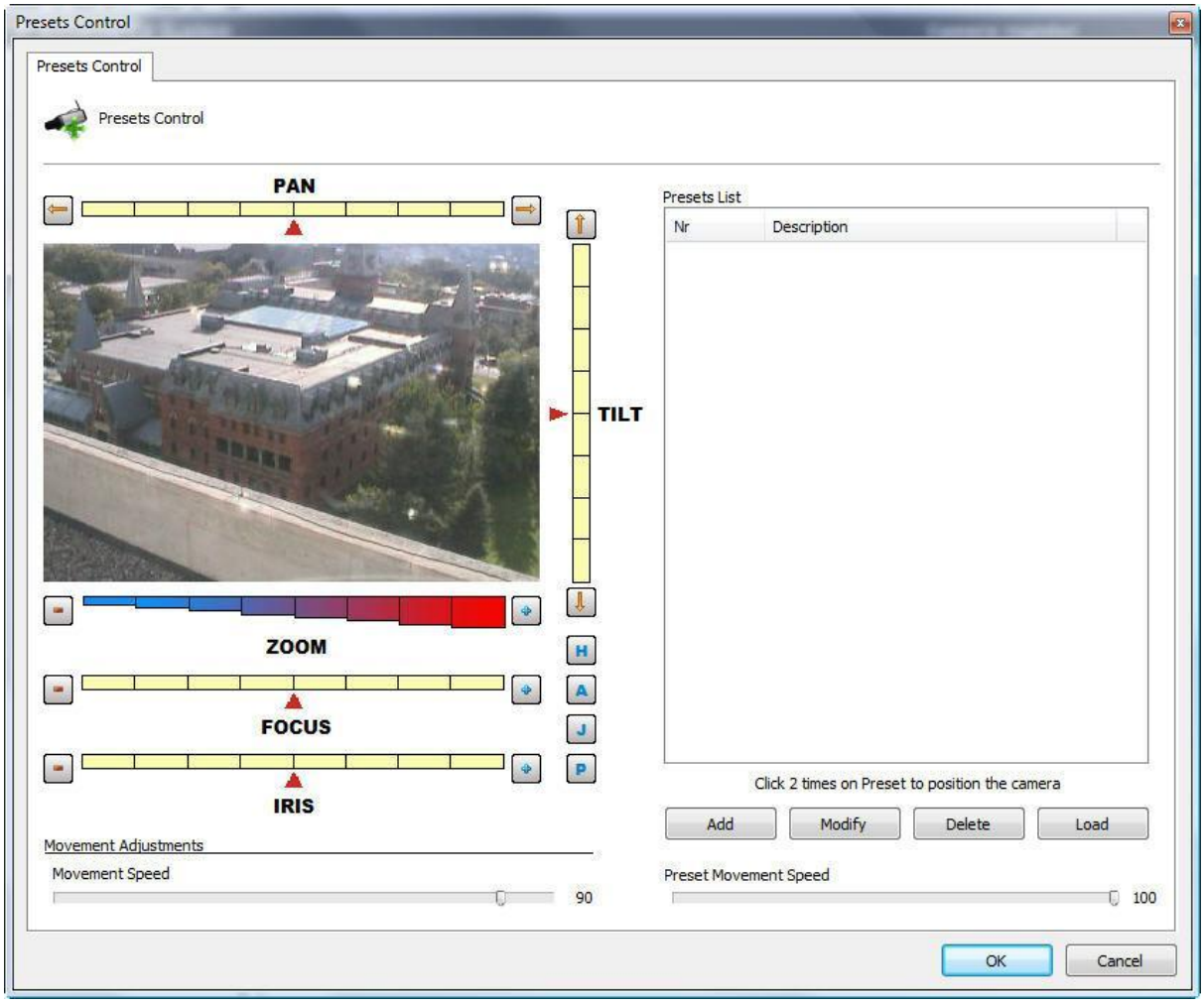
Each model of camera supports a certain number of presets. The role of Digifort is to maintain an internal positions list created by the user referring to the list of internal presets of the camera, that is, the position 1, created by the user, is associated to internal position 1 of the camera, for example. When the user adds a preset, the two positions are linked.

The presets will be available for use in the Surveillance Client. Consult the Surveillance Client to learn how to call up the configured preset.

To access this feature, click on the Presets Control button, opening the screen

© 2002 - 2011 by Optiview USA all rights

below:



- **PAN bar**: Moves the camera to the left and to the right
- **TILT bar**: Moves the camera up and down
- **ZOOM bar**: Moves the camera's zoom in and out.
- **Focus bar**: Adjusts the camera's focus, in case this isn't done automatically.
- **Iris bar**: Adjusts the camera's iris, in case this isn't done automatically.
- **Home button**: This configuration is located on the button identified by an "H". Clicking on this button causes the camera to be positioned in its initial factory-determined position.
- **Advanced PTZ button**: This configuration is located on the button identified by an "A". Clicking on this button causes the advanced PTZ controls to be displayed. To learn how to use this feature, see Advanced PTZ.
- **Visual Joystick button**: This configuration is located on the button identified by a "J". Clicking on this button causes the visual joystick to be displayed over the allowing you to control its movement by mouse. To learn how to use this feature, see page Visual Joystick.
- **Movement adjustments**:
  - **PTZ by bar**:Define in what way the new camera positioning will be obtained. This configuration can have one of two values:
    - **Absolute PTZ**: The new positioning commands of the camera will be

© 2002 - 2011 by Optiview USA all rights

absolute, that is, relative to the Home position..

§ **Relative PTZ**: The new positioning commands of the camera will be relative to the present position

○ **Movement speed:** Movement speed of the camera while its position is being adjusted. This value is expressed as a percentage and its default value is 90% of the maximum speed of the camera.

- **Presets list:** This list contains all of the presets registered for this camera. To position the camera in a preset, double-click on the preset.
- **Add button:** Memorizes the present position of the camera. To learn how to use this feature, see How to create a preset
- **Modify button:** Modifies the selected preset..
- **Exclude button**: Excludes the selected preset.
- **Download button**: Loads the configured camera presets directly to the camera.
- **Preset movement speed**: Specifies the movement speed of the camera from one preset to another. This value is expressed as a percentage and its default value is 100% of the maximum speed.

Important

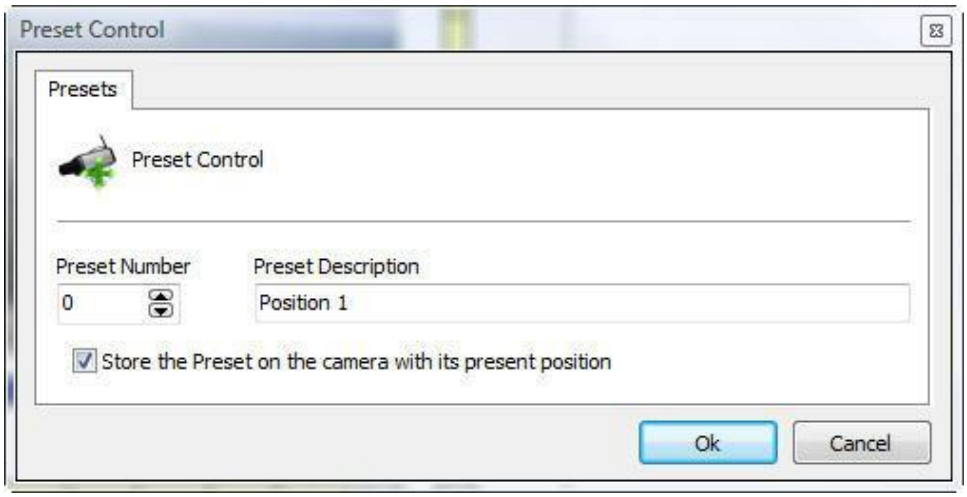
The presets list shows only a list of presets belonging to the camera. All presets created by Digifort are saved in the camera itself. Digifort associates the item of the list with the preset of the camera by way of its number.

Tip

it's possible to position the camera merely by clicking on the image in the place in which you wish to centralize it or use a table joystick.

6.1.5.9 How to create a preset

The process of creation of presets is quite easy, simply positioning the camera with the controls presented in the previous topic and clicking on Add, as shown in the picture below:



- **Preset number:** The number of the preset that Digifort will associate with the

© 2002 - 2011 by Optiview USA all rights

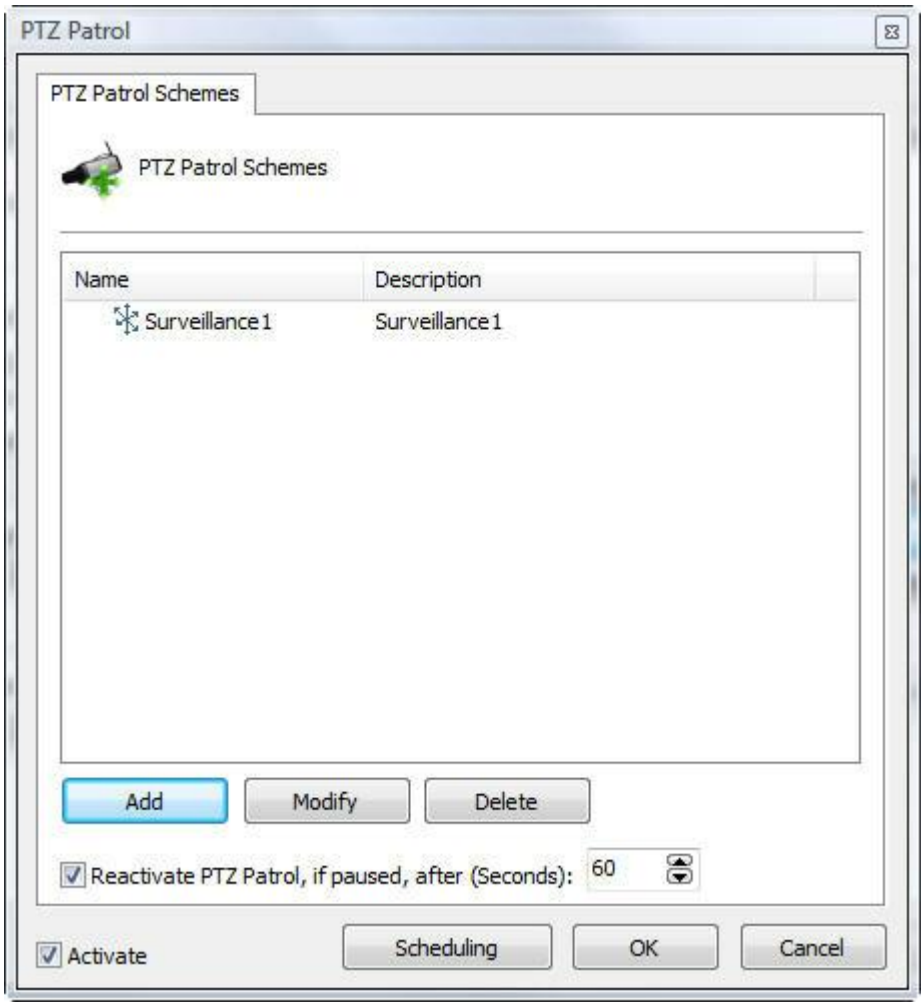
camera's internal presets list.

- **Description of the preset:** A description of the preset being added. This name will be displayed to the user in the Surveillance Client.
- **Record the preset in the camera with its present position:** With this option marked, Digifort will substitute the position of the camera of the informed preset number. In the example of the picture above, the position of the camera will be saved in the preset number zero of the camera. With this option unmarked, Digifort will only associate the description of the preset with the present position of the camera of preset zero..

6.1.5.10 How to configure PTZ Patrol

PTZ Patrol is a feature available in Digifort where it's possible to make the camera pass through the presets previously registered in the system.

To access this feature, click on **PTZ Patrol**, opening the screen below:



- **Scheme list:** List of PTZ patrol schemes created for the selected camera.
- **Add button**: Adds a new PTZ patrol scheme

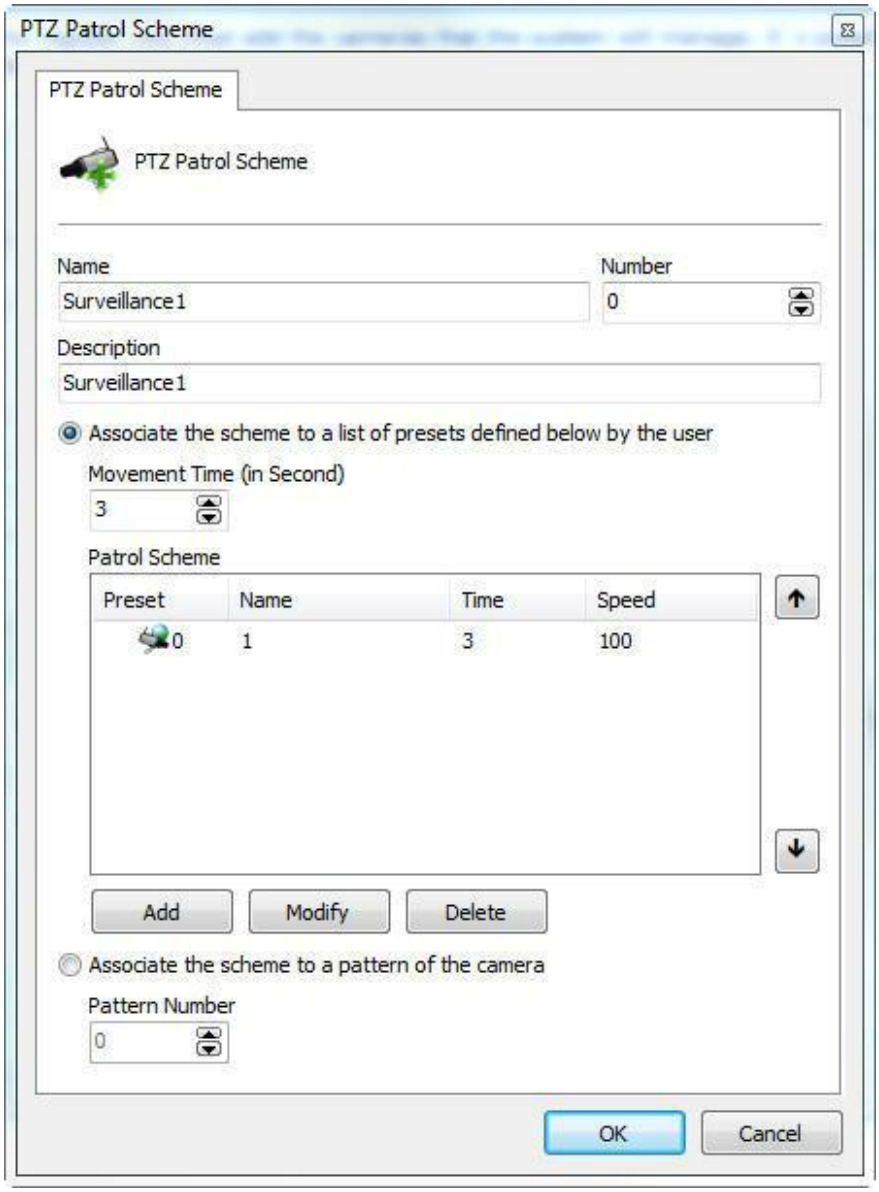
© 2002 - 2011 by Optiview USA all rights

- **Modify button:** Modifies the selected scheme.
- **Exclude button:** Excludes the selected scheme
- **Reactivate PTZ patrol, if paused, after (seconds):** Reactivates the PTZ patrol in the specified time if it was paused in the Surveillance Client.
- **Activate**: Activates the PTZ patrol scheme.
- Scheduling button: Defines times of day and days of the week in which the PTZ schemes will work. To learn how to use this feature, see : Defines times of day and days of the week in which the PTZ schemes will work. To learn how to use this feature, see How to configure the scheduling of PTZ Patrol schemes

6.1.5.10.1 How to add a PTZ Patrol scheme

After clicking on the **Add** button, as explained in the previous topic, the screen below will be displayed:

© 2002 - 2011 by Optiview USA all rights



· **Name of the scheme:** Inform the identification name of the PTZ patrol to be created.
· **Description of the scheme**: Inform a short description of the PTZ patrol to be created.
· **Associate the scheme with the list of presets defined below by user:** Allows the user to create the list of presets in which the camera will position itself during PTZ patrol.
  o **Movement time:** Inform the average movement time of the camera from one position to another.
  o **Patrol scheme:** List of presets added by the user.
  o **Add button:** Adds a preset to the scheme to be created.
  o **Modify button:** Modifies the selected preset.
  o **Exclude button:** Excludes the selected preset.
· **Associate the scheme to a camera pattern:** Select this option if the Recording Server PTZ patrol is configured directly in the camera. To learn

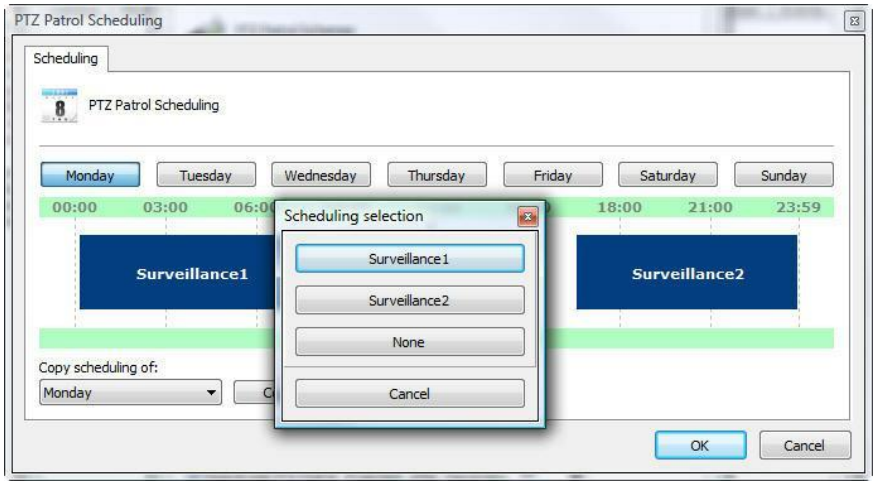
© 2002 - 2011 by Optiview USA all rights

how to use this
feature, consult the manual of your camera.
o Pattern number: Number of the pattern configured in the camera.

6.1.5.10.2 How to configure the scheduling of PTZ Patrol schemes

After registering all of the PTZ patrol schemes, it's necessary to define the hours and days of the week in which these schemes will enter into effect.

To configure the scheduling, click on the Scheduling button, as shown in the picture below



In the example of the picture above, the following scheduling was configured:

- **00:00 to 06:00:** The scheme Tour enters into effect.
- **06:01 to 12:00:** No scheme enters into effect, at this moment the camera becomes fixed.
- **12:01 to 18:00:** The scheme Patrol enters into effect.
- **18:01 to 21:00:** No scheme enters into effect, at this moment the camera becomes fixed.
- **21:01 to 23:59:** In this time range, a new scheme is being configured.

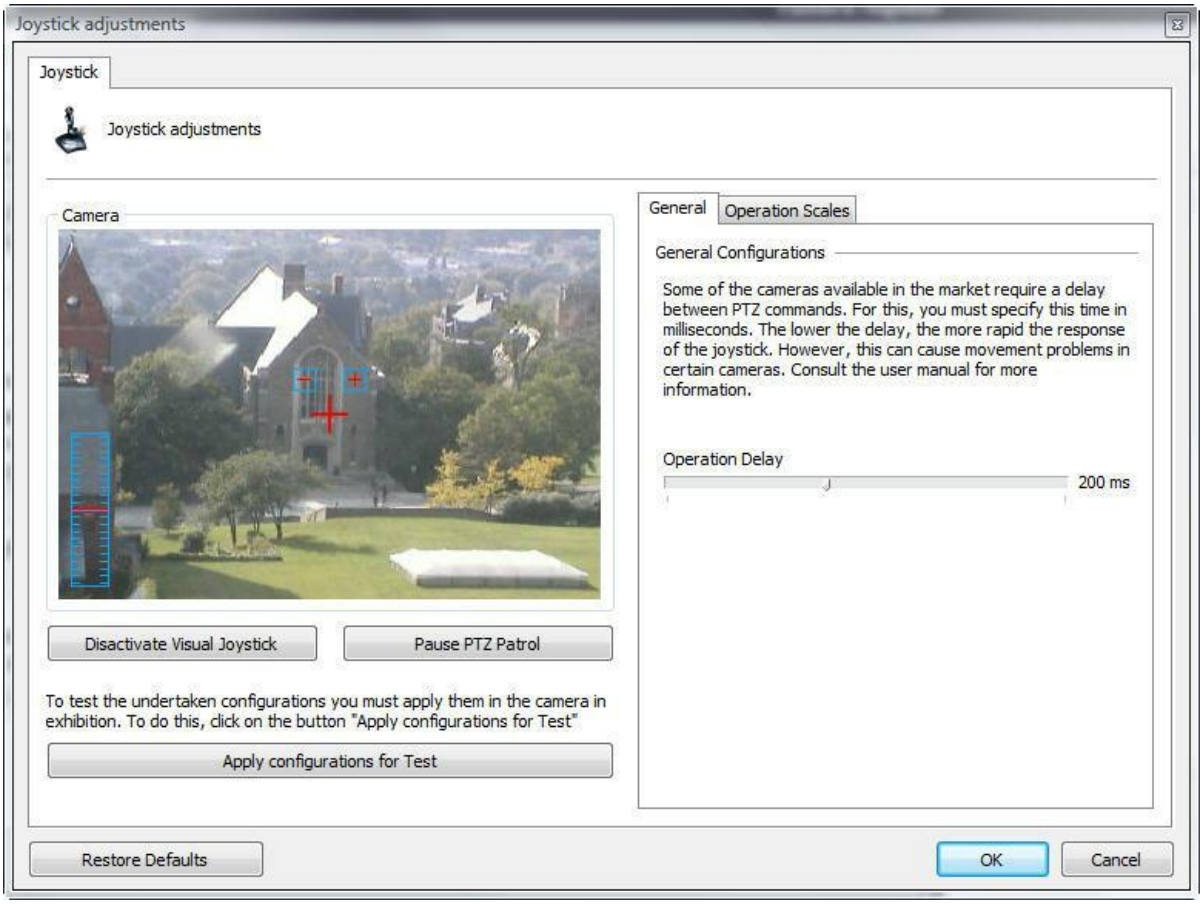
6.1.5.10.3 How to configure the Joystick

The joystick configurations allow its adjustment, aimed at customizing the operating method according to the user's taste.

These configurations involve parameters such as the sensitivity of the joystick and delay of operation.

To access this configuration, click on the **Joystick Configurations** button, located in the PTZ configurations of the camera, opening the screen below:

© 2002 - 2011 by Optiview USA all rights


Joystick adjustments
Joystick
Joystick adjustments
Camera
General
Operation Scales
General Configurations
Some of the cameras available in the market require a delay between PTZ commands. For this, you must specify this time in milliseconds. The lower the delay, the more rapid the response of the joystick. However, this can cause movement problems in certain cameras. Consult the user manual for more information.
Operation Delay
200 ms
Disactivate Visual Joystick
Pause PTZ Patrol
To test the undertaken configurations you must apply them in the camera in exhibition. To do this, click on the button "Apply configurations for Test"
Apply configurations for Test
Restore Defaults
OK
Cancel

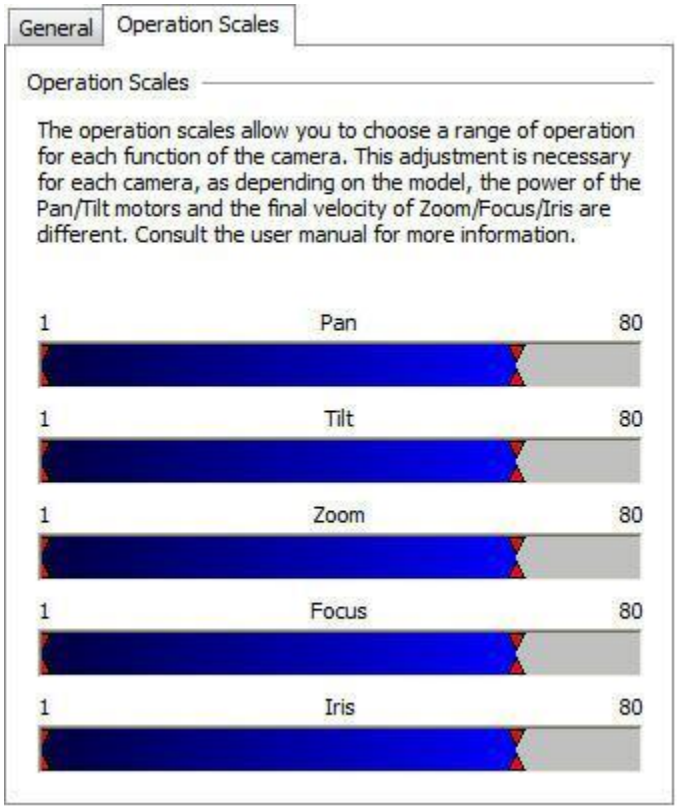
- **Disactivate the visual joystick**: Disactivates the visual joystick. To learn how the visual joystick works, see Visual Joystick.
- **Apply configurations for test**: Applies the prepared configurations only for test. The tests of camera movement with the prepared adjustments should be done on the camera image in the configuration screen itself.
- **Restore Defaults button**: Restores the default configurations of the joystick adjustments.
- **General tab**: Allows access to the configurations of delay of operation.
- **Operation Scales tab:** Allows access to the configurations of the operation scales, defining the sensitivity for the joystick.

The delay of operation is the system's wait time for the command to be sent to the camera. The default of this configuration is 200ms, that is, moving the joystick to the left and holding it in this position for 200ms, the command will be sent to the camera, for example.

The operation scales allow you to choose an operation range for each function of the camera. All of the values are expressed in percentages.

To access this feature, click on the Operation Scales tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



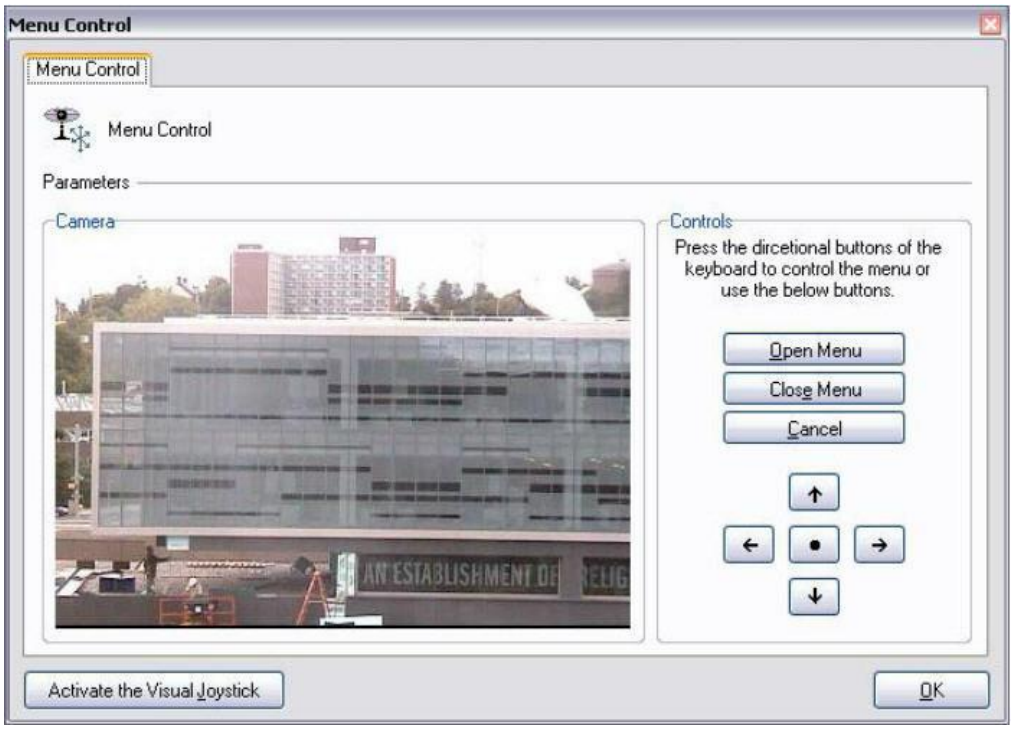
These configurations are applied to the force of the motors. For a better understanding of this configuration, let's look at the PAN bar. If you hold the joystick all the way to the left, the speed of the camera will be 80% of its maximum speed. It's also possible to specify a minimum movement speed, that is, if you hold the joystick only a few centimeters to the left, the speed of the camera will be 5% of the minimum speed of the camera.

6.1.5.10.3.1 How to remotely configure analogical cameras

Digifort allows the remote configuration of analogical cameras. This configuration is very useful when we have a camera of difficult access and it's necessary to execute its configuration.

To access this configuration, click on the Open Menu Control button, located in the PTZ configurations of the camera, opening the screen below:

© 2002 - 2011 by Optiview USA all rights



- **Open Menu button**: Opens the configurations menu of the camera.
- **Close Menu button:** Closes the configurations menu of the camera.
- **Navigation button:** Navigates through the configurations menu of the camera. Click on the central button to enter in a configuration.
- **Activate the Visual Joystick button**: Activates the visual joystick. To learn how the visual joystick works, see Visual Joystick

The visual joystick is a tool that simulates the functions of a table joystick. Upon activating the visual joystick over a camera, it will have the appearance of the picture below:



© 2002 - 2011 by Optiview USA all rights

To use the visual joystick, keep the left button of the mouse clicked and move it to any position on the image. The further the mouse is kept from the center of the image, the faster the movement of the camera will be, and vice-versa.

To carry out zoom operation, use the wheel of the mouse, turning it to front, the image will be brought closer, and to the back pushes the image away. The speed of the zoom can also be controlled and visualized by the control at the left side of the image. The closer the red mark is to the center, the faster the zoom, and vice-versa.

The sensitivity of movement and zoom can be adjusted in the operation scales configurations on page How to configure the Joystick

Digifort is equipped with a tool that makes it possible to control the movement of a PTZ camera in a detailed way. This tool is called Advanced PTZ.

To access this feature, click on Advanced PTZ, identified by an “A” in the register of camera presets, displaying the screen below:

© 2002 - 2011 by Optiview USA all rights



- Focus control: Manually adjusts the focus of the camera.
- **Iris control:** Manually adjusts the opening of the camera's iris.
- **Operation factor:** This value is expressed in percentage and defines the speed of the focus and iris motors to be moved in the camera. If in 50, the camera will move at 50% of its maximum speed, for example.
- **Activate Auto-Focus button**: Activates the camera's automatic

© 2002 - 2011 by Optiview USA all rights

focussing, if this exists.

- **Disactivate Auto-Focus button:** Disactivates the camera's automatic focussing, if this exists.
- **Activate Auto-Iris button:** Activates the camera's automatic iris control, if this exists.
- **Disactivate Auto-Iris button**: Disactivates the camera's automatic iris control, if this exists.
- **Activate Wiper button:** Activates the camera's wiper.
- **Disactivate Wiper button:** Disactivates the camera's wiper.
- **Home Position button:** Positions the camera in its factory-configured initial position.
- **Relative PTZ:** Moves the camera in relation to its current position.
  - **Pan:** Moves the camera to the left and to the right in relation to its current position.
  - **Tilt:** Moves the camera up and down in relation to its current position.
  - **Zoom:** Moves the camera's zoom forwards and backwards in relation to its current position.
  - **Focus:** Adjusts the camera's focus in relation to its current adjustment.
  - **Iris:** Adjusts the opening of the camera's iris opening in relation to its current opening

- **Absolute PTZ:** Moves the camera in relation to the home position.
  - **Pan**: Moves the camera to the left and to the right in relation to its home position.
  - **Tilt**: Moves the camera up and down in relation to its home position.
  - **Zoom:** Moves the camera's zoom forwards and backwards in relation to its home.
  - **Focus:** Adjusts the camera's focus in relation to its home adjustment.
  - **Iris:** Adjusts the opening of the camera's iris opening in relation to its home opening.

- **Operation factor:** This value is expressed in percentage and defines the speed of the PTZ motors to be moved in the camera. If in 80, the camera will move at 80% of its maximum speed, for example.

- **Close button**: Closes the Advanced PTZ screen.

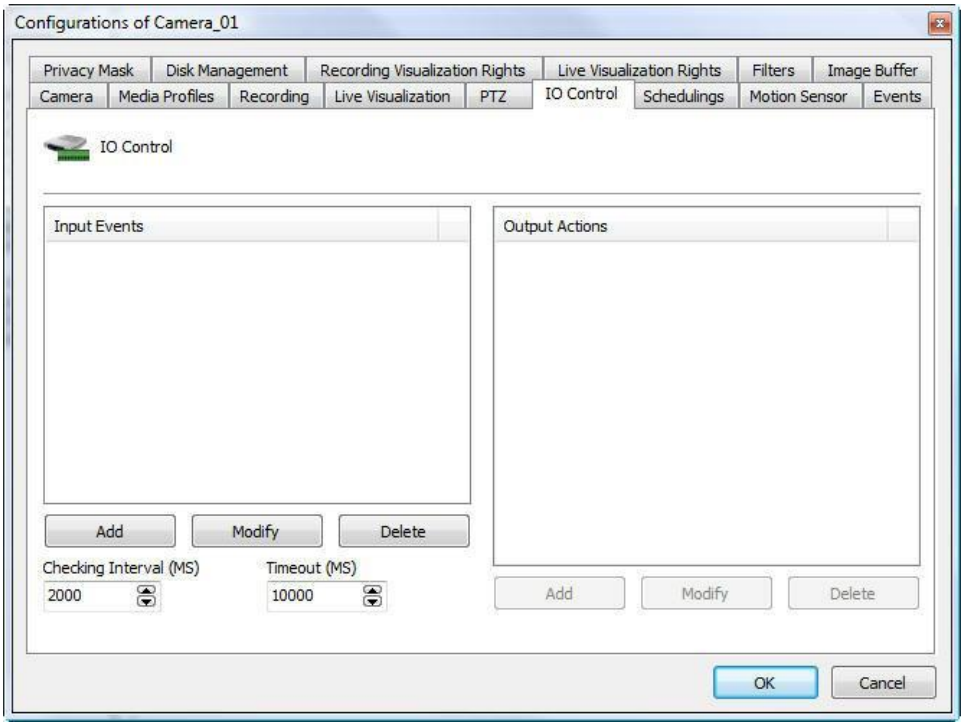
6.1.6 How to configure the I/O

Digifort is able to control the alarm inputs and outputs of cameras that have this feature.

An I/O input could be, for example, a presence sensor, and an I/O output could be, for example, a siren or an electric lock.

To access this feature, click on the **I/O Control** tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



- **List of Input Events**: Displays all of the input events of a camera.
- **List of Output Actions**: Displays all of the output events of a camera.
- **Checking Interval (ms)**: Interval in which Digifort communicates with the camera to recognize some input event, for example, a presence sensor.
- **Timeout (ms):** Interval after which Digifort will try a new connection with the camera in case the present connection is lost.

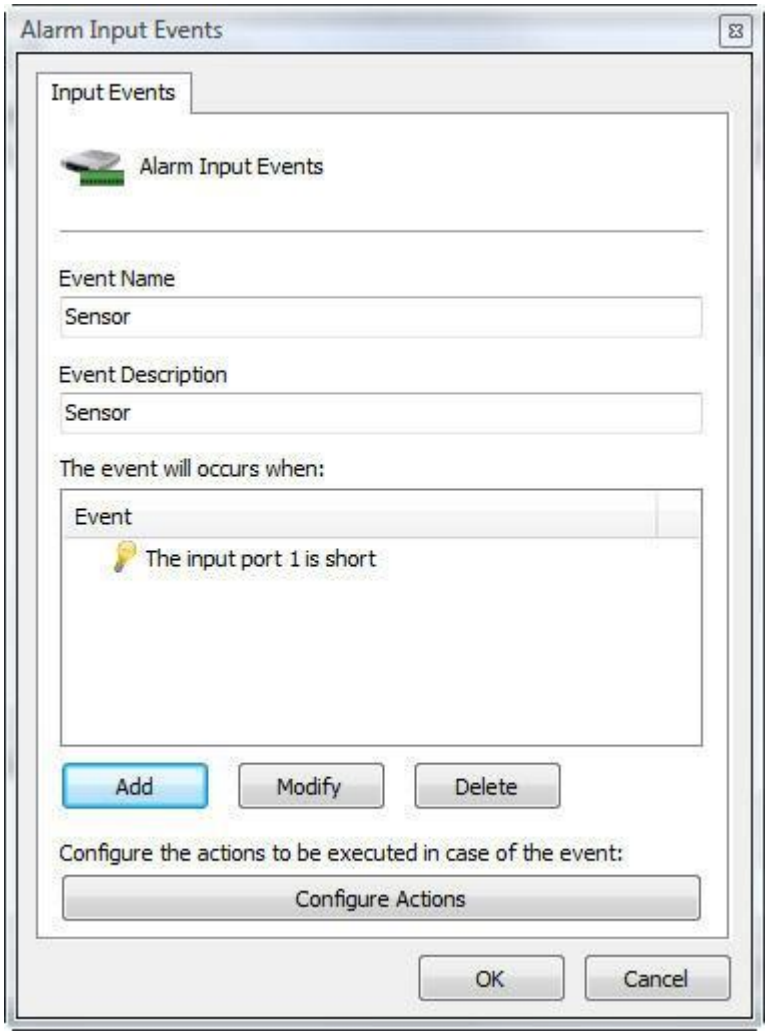
6.1.6.1 How to add input events

To add an input event, click on **Add**. To modify and input event, click on **Modify**.

To exclude and input event, click on Exclude. All of these buttons refer to the input events located right below its list.

After clicking on **Add**, the following screen will be displayed:

© 2002 - 2011 by Optiview USA all rights



- **Event name:** Name of the camera input event.
- **Description of this event:** Description of the camera input event.
- **The event will occur when:** Fill in the list according to your needs. In the example above, the configuration is for the event to be generated only when port 1 of the camera alarm input is activated. Combinations can be created, such as port 1 activated, 2 activated and 3 disactivated. To add an event click on the **Add** button. To modify and exclude, click on the corresponding buttons. After clicking on the **Add** button, the following screen will be displayed:

© 2002 - 2011 by Optiview USA all rights



In this screen, select the input port and its state for which the event being configured occurs.

- **Configure Actions button:** Click on this button to configure the actions that Digifort will execute when this event happens. To learn how to configure the actions, see How to configure the alarm actions.

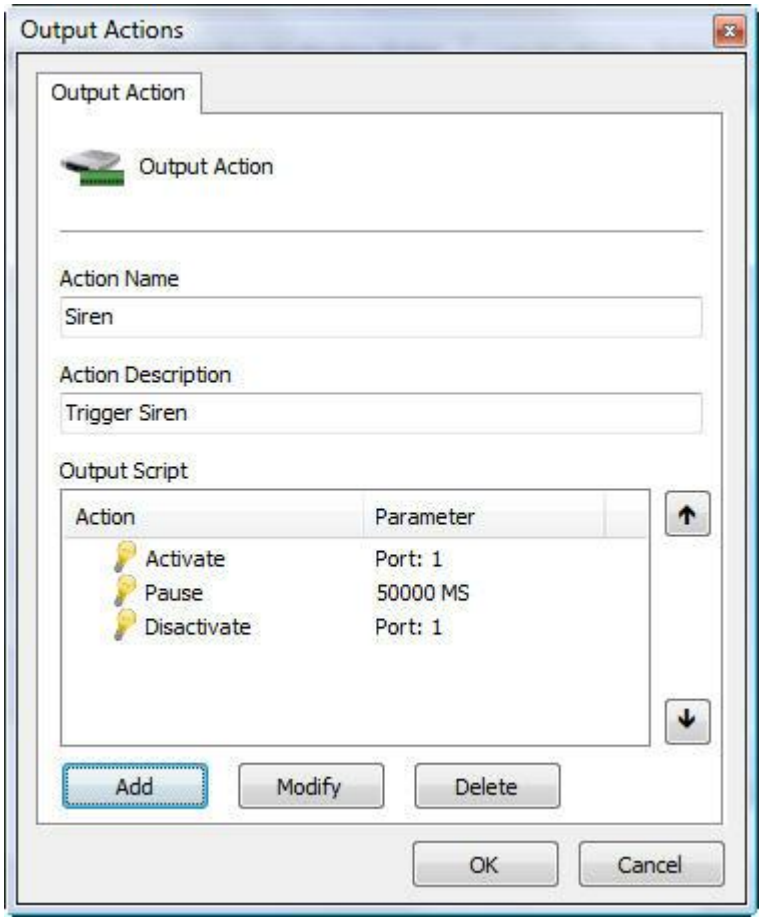
6.1.6.2 How to add output events

The output events of a camera are configured in the form of script, that is, a set of parameters that are executed in the order defined by the user.

To add an output event, click on **Add**. To modify an output event, click on Modify. To exclude an output event, click on Exclude. All of these buttons refer to the output events located right below its list.

After clicking on **Add**, the following screen will be displayed:

© 2002 - 2011 by Optiview USA all rights



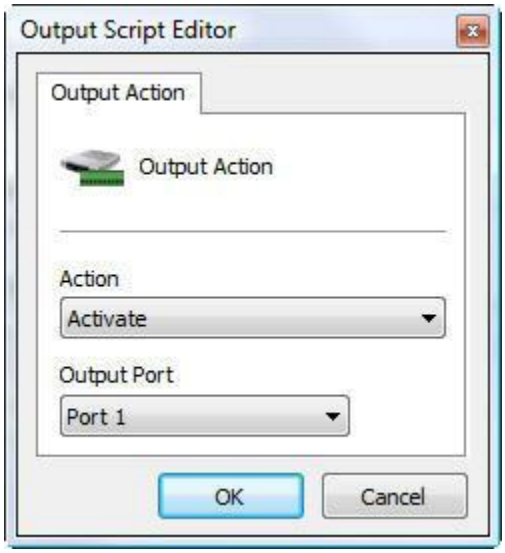
- **Action name**: Enter the name of the output action
- **Description of this action**: Enter the description of this output action.
- **Script for output**: Displays the list of parameters to be executed in this event. In the picture above, we have the example of the sounding of a siren in the following way:

1. Turn on the siren
2. Keep the siren turned on for 50 seconds (50000 ms)
3. Turn off the siren

To add an output action, click on **Add**. To modify or exclude, click on the corresponding button.

After clicking on **Add**, the following screen will be displayed:

© 2002 - 2011 by Optiview USA all rights



In this screen, select the action and the port in which the action will be executed.

6.1.7 How to configure schedulings

Schedulings are tools that make it possible to configure the times of day and days of the week for certain Digifort events to be recognized.
By default, any scheduling is already configured to recognize events 24 hours per day and 7 days per week.

In the Enterprise version of Digifort, configurations are available for schedulings of recording, transmission, and events.

The scheduling of recording allows the selection of times of day and days of the week in which the camera will be continuously recorded, recorded by motion detection, or recording by event. This configuration will only be available if the type of recording is configured to use scheduling of recording.

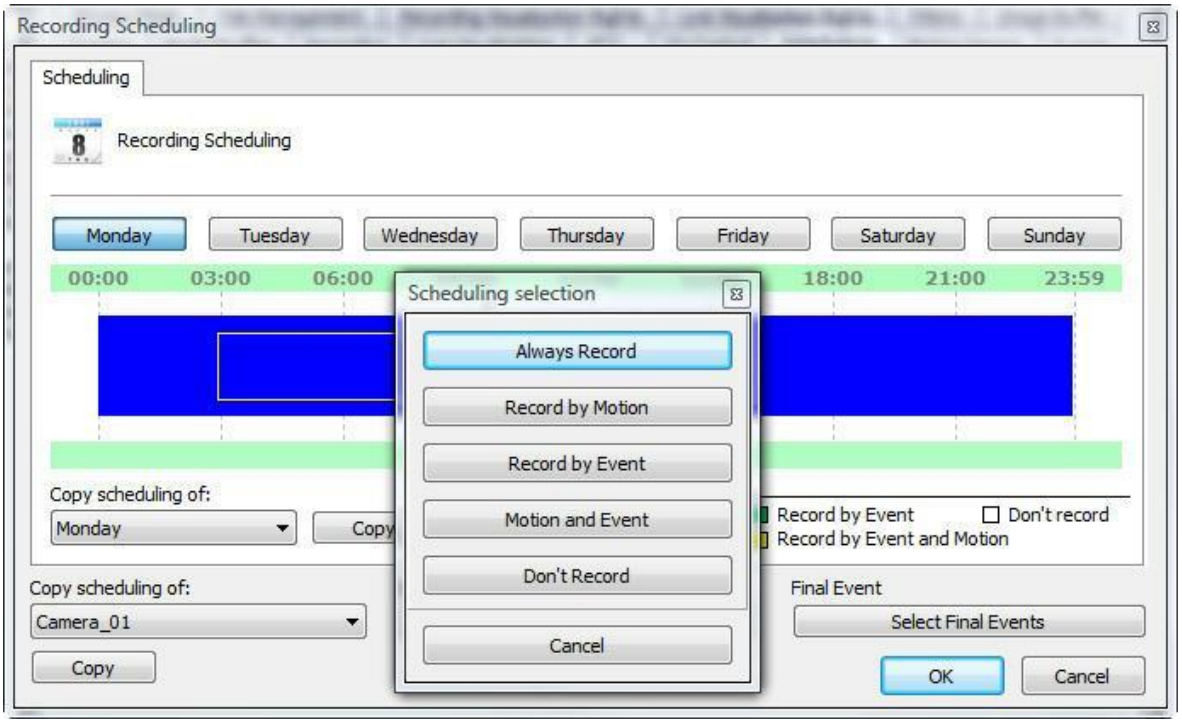
The scheduling of transmission allows the selection of times of day and days of the week in which the Digifort Server will receive images from the cameras, whereby it's possible to transmit only upon detection of events or never transmit. This scheduling can help in the saving of network bandwidth.

The scheduling of events allows the selection of times of day and days of the week in which the Digifort Server will recognize the events registered in the system such as, for example, the motion detection by way of a presence sensor.

6.1.7.1 How to configure the scheduling of recording

To configure the scheduling of recording, click on the Open Scheduling of Recording button, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



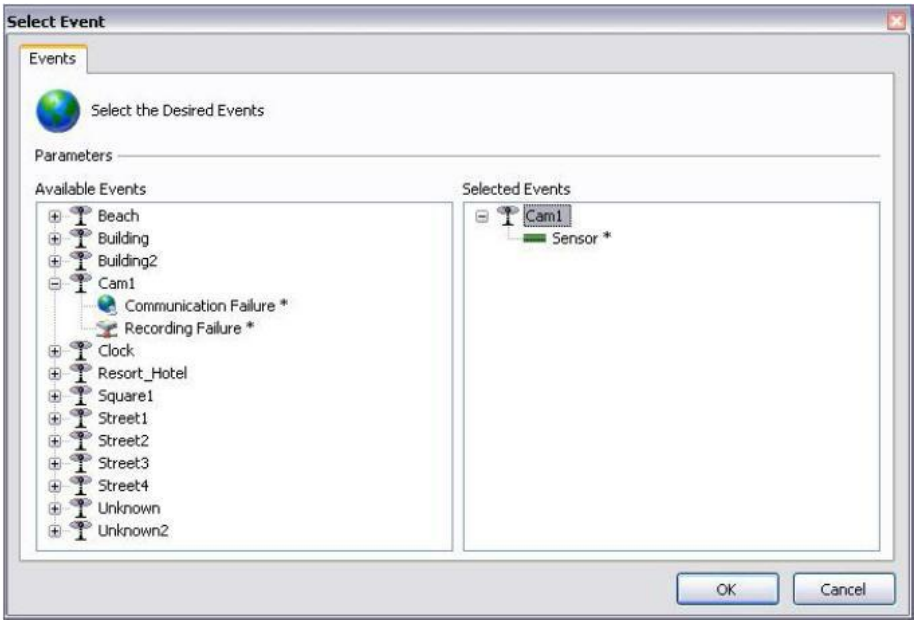
The functioning of this screen is quite simple. In the upper part of the screen we have the buttons corresponding to the days of the week, in the center part we have the buttons corresponding to the hours of the day, and in the lower part we have the controls for copying of schedulings and the legend.

To create a scheduling, select the day of the week and keep the left button of the mouse pressed over some hour and drag it to the other hour, forming a rectangle. After this action, a window will be opened, requesting the type of scheduling to be created. Select the most convenient action. The options for scheduling are:

- **Always record:** Activates the continuous recording of the camera during the specified hours. This option is represented in blue.
- **Record by motion**: Activates the recording by motion in the camera during the specified time. This option is represented in red. To learn about recording by motion, see How to configure the Motion Sensor
- **Record by event:** Activates the recording by event in the camera during the specified time. This option is represented in green.
- **Motion and event**: Activates the recording by motion detection and by detection of camera events. This option is represented in yellow. To learn about motion detection, see How to configure the Motion Sensor.
- **No recording:** Disactivates the recording of the camera during the specified time. This option is represented in white.
- **Cancel:** Cancels the creation of scheduling during the specified hours.
- **Select Initial and Final Events button:** If the type of scheduling is configured to record by event, click on this button to configure the event that starts or ends the recording of images from the camera in the server.

© 2002 - 2011 by Optiview USA all rights

After clicking on this button, the following screen will be displayed:



This screen presents two lists, the list of available events and the list of selected events.

The list of available events displays the list of all cameras and alarm devices registered in the system, and the list of selected events displays all of the events that are added by the user so that the event occurs.

The events that have an "*" at the side are the events that in fact will occur, that is, supposing that we have timer-linked events. In this case not all of the events will occur, but those that have an "*" at the side. Timer events are those that occur in at a determined time defined by the user to touch off another event. To learn about timer events, see Timer Events.

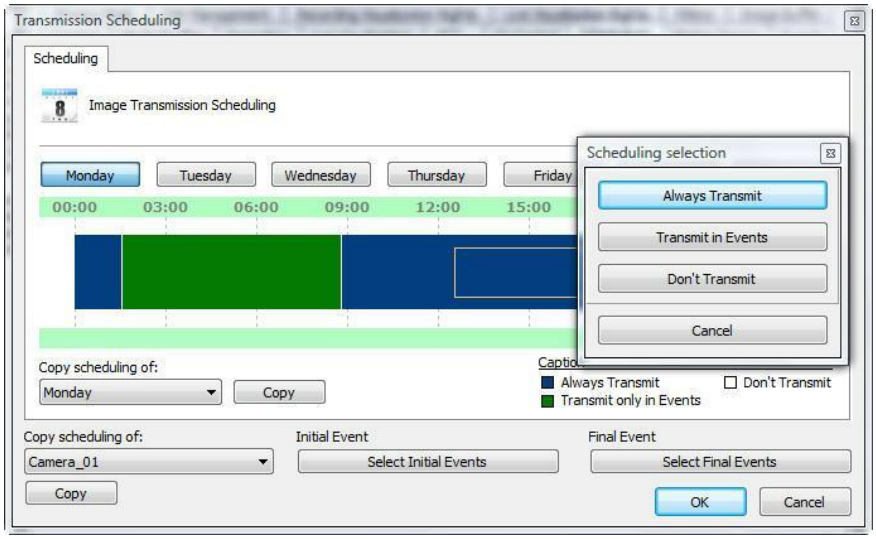
To select an event, select it in the list of available events and drag it to the list of selected events. To remove an event, do the same process in reverse.

After the creation of schedulings for a day of the week, it's possible to copy it to other days that are to have the same configuration, by simply selecting the desired day of the week in the field Copy Secheduling of and pressing the Copy button.

6.1.7.2 How to configure the scheduling of transmission

To configure the scheduling of transmission, click on the **Open Scheduling of Transmission** button, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights

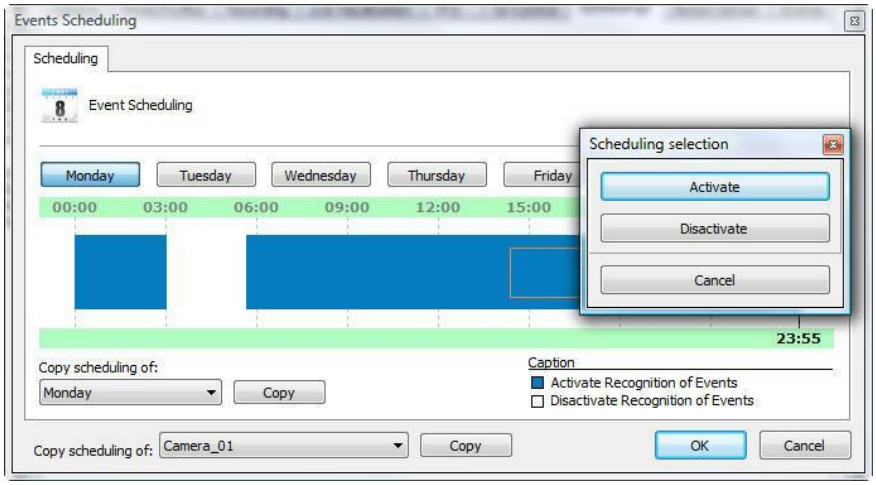


The functioning of this screen is identical to the screen specified in the previous topic, except for the types of schedulings:

- **Always transmit:** Always transmits the camera images during the selected time and day of the week. This option is represented by blue.
- **Transmit by events:** Transmits the camera images when events occur during the configured initial and final times. This option is represented by green.
- **No transmission**: Never transmits camera images in the specified hours and days. This option is represented by white.
- **Select initial and final events button:** If the type of transmission is configured for transmission by event, click on this button to configure the event that will start or end the transmission of camera images to the server and follow the instructions presented in the previous topic.

6.1.7.3 How to configure the scheduling of events

To configure the scheduling of events, click on the Open Scheduling of Events button, as shown in the picture below:



© 2002 - 2011 by Optiview USA all rights

The functioning of this screen is identical to the screen specified in the previous topic, except for the types of schedulings:

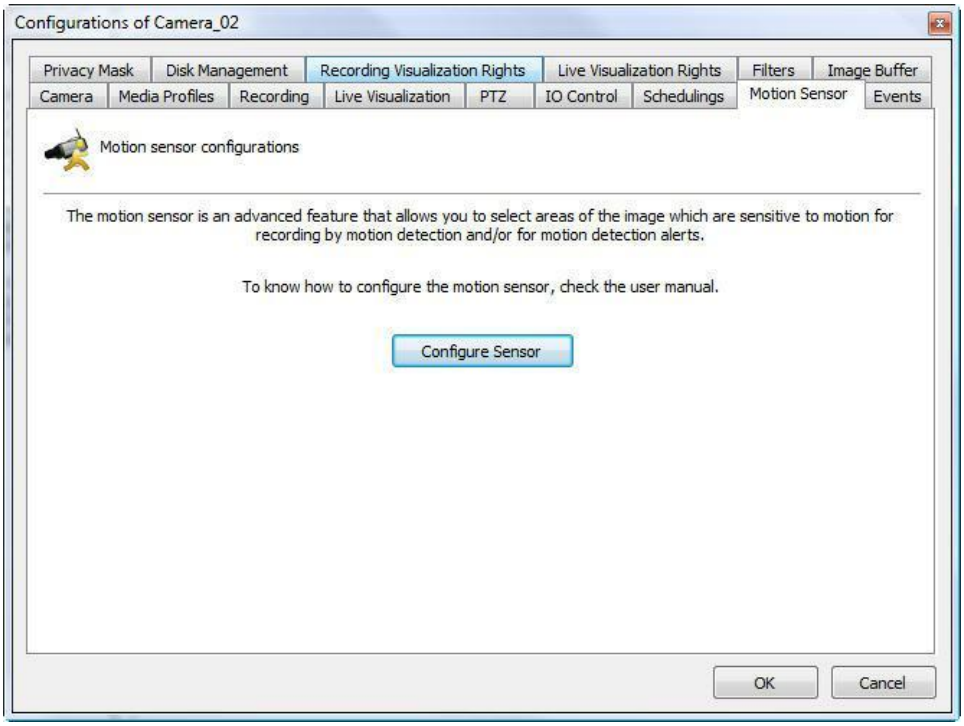
- **Activate**: Activates the recognition of events of this camera in the specified hours and days of the week. This option is represented by blue.
- **Disactivate**: Disactivates the recognition of events of this camera in the specified hours and days of the week. This option is represented by white.

6.1.8 How to configure the Motion Sensor

The Motion Sensor is a tool which makes it possible for the user to define areas of the image that will be sensitive or insensitive to motion.

The configuration of the motion sensor is very important for the saving of disk space used by the camera. If you selected the method of recording by **motion detection** in the **Camera** tab, it's recommended that you adjust the sensor according to your needs.

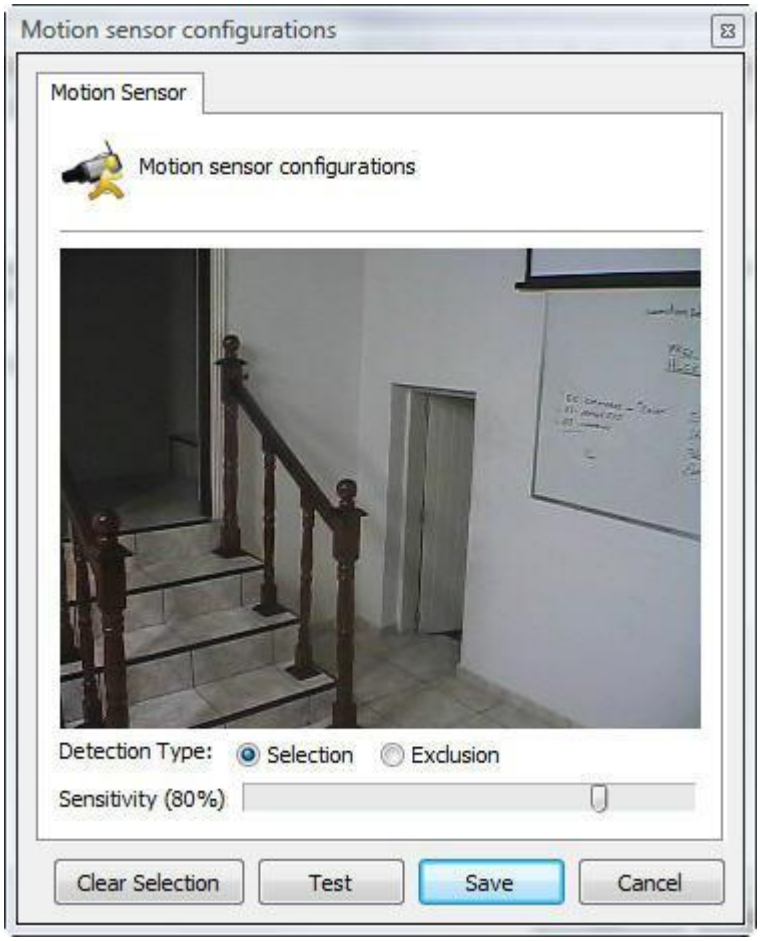
As default, if the sensor is not configured, the entire image will be sensitive to motion.
To access this feature, click on the **Motion Sensor** tab, as shown in the picture below:



To configure the motion sensor, click on the Configure **Sensor Button**.

After clicking on this button, the motion sensor configuration window will open with a real image from the camera, as can be seen in the picture below:

© 2002 - 2011 by Optiview USA all rights



In this screen, you will be able to select the areas that will be sensitive to motion or areas will not be sensitive to motion.

To select areas that will be sensitive to motion, select the detection type Selection a click on the image, dragging the mouse to form a selection box. To select areas that will not be sensitive to motion, select the button Exclusion, repeating the process.

To exclude already configured areas, click on the right button of the mouse and select the box to be excluded or click on the Eliminate Selection button to eliminate all of the defined areas.

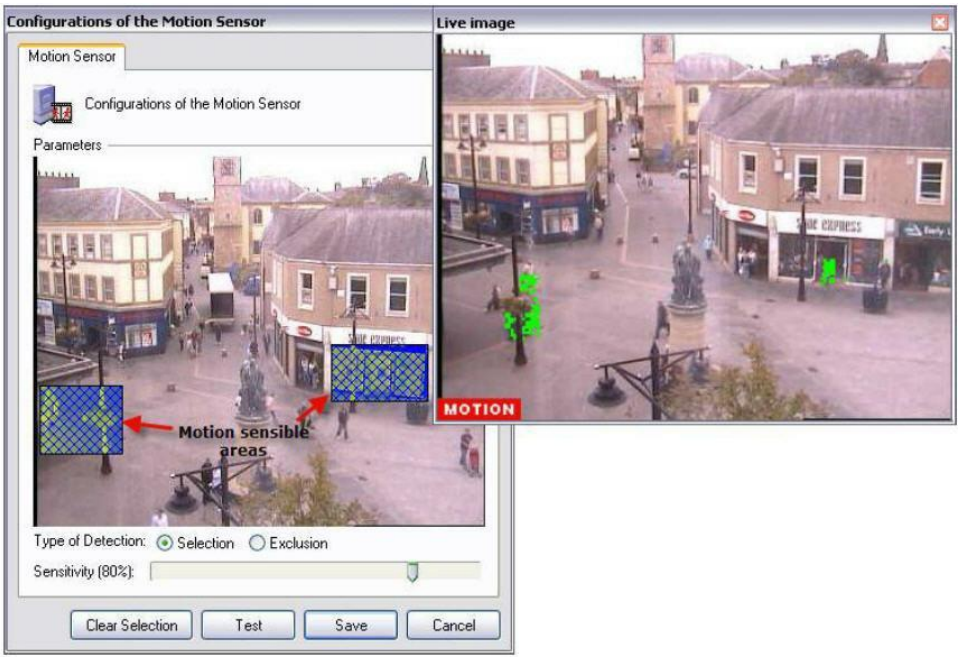
After selection of the desired areas, configure the sensitivity of motion. As default, the sensitivity is 80%. With this value, it's already possible to detect any type of motion in the image.

Once this is done, click on the Test button to visualize the functioning of the selected motion detection.
For performance reasons, Digifort analyses the camera images at two frames per second, that is, it's not necessary to detect motion in all of the frames, but only to analyze an image every 500ms. With this default any type of movement

© 2002 - 2011 by Optiview USA all rights

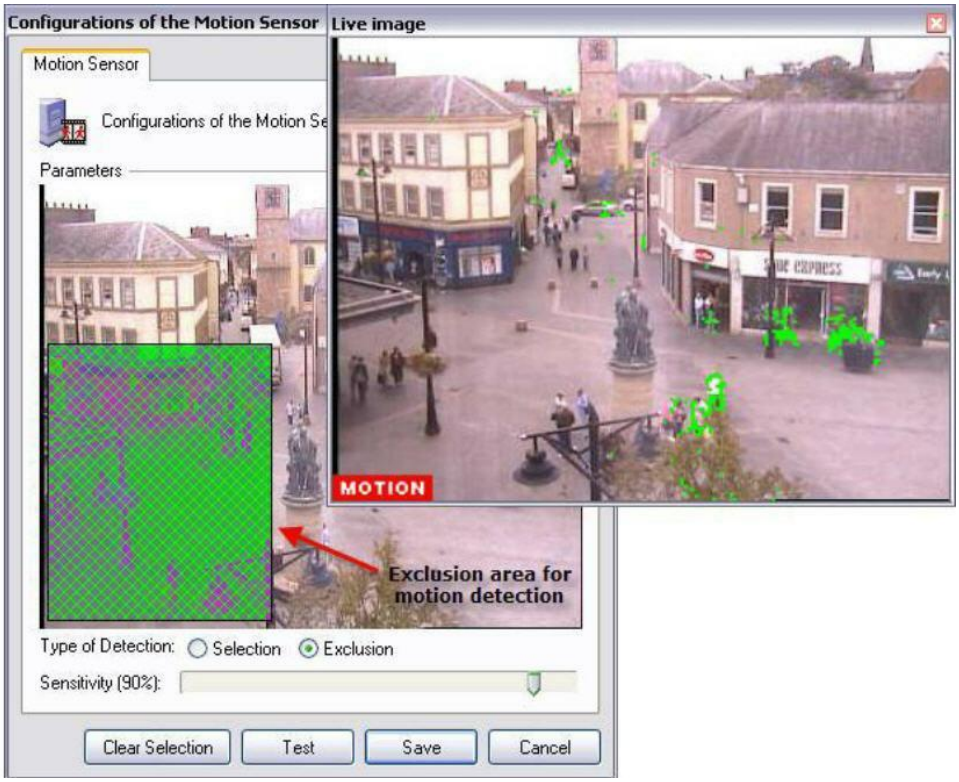
is detected.

The picture below demonstrates the workings of the motion sensor with selection of areas sensitive to motion:



The picture below: demonstrates the workings of the motion sensor with selection of areas not sensitive to motion:

© 2002 - 2011 by Optiview USA all rights

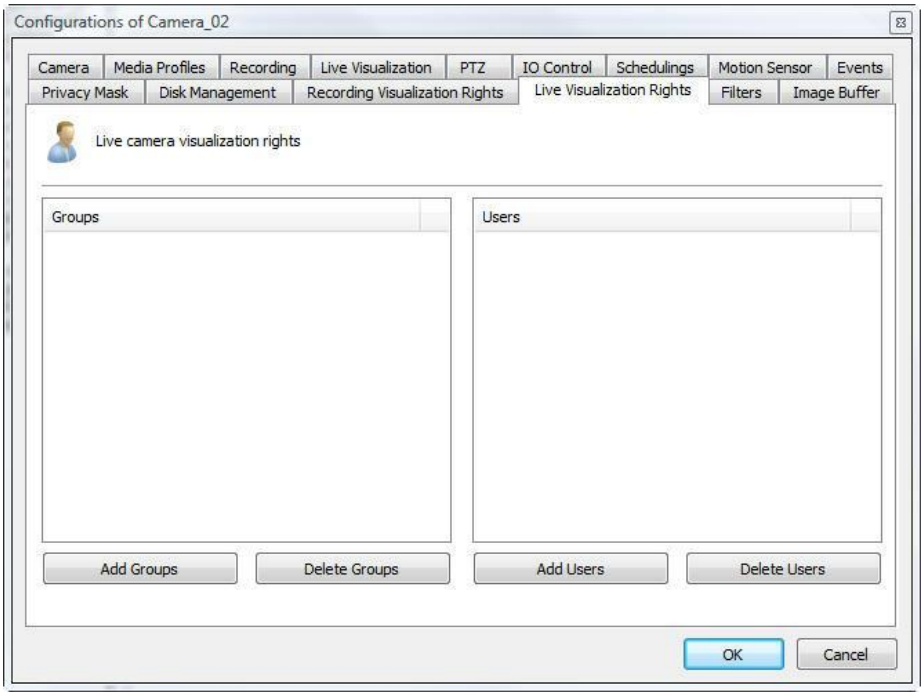


6.1.9 How to configure the recording visualization rights

This area of the camera register is reserved for the definition of the rights of visualization of recordings, that is, which users will be able to see videos already stored in the server, as opposed to live visualization rights, where which users are able to visualize cameras in real time are defined.

To access this feature, click on the Recording Visualization Rights tab, as shown in the picture below:

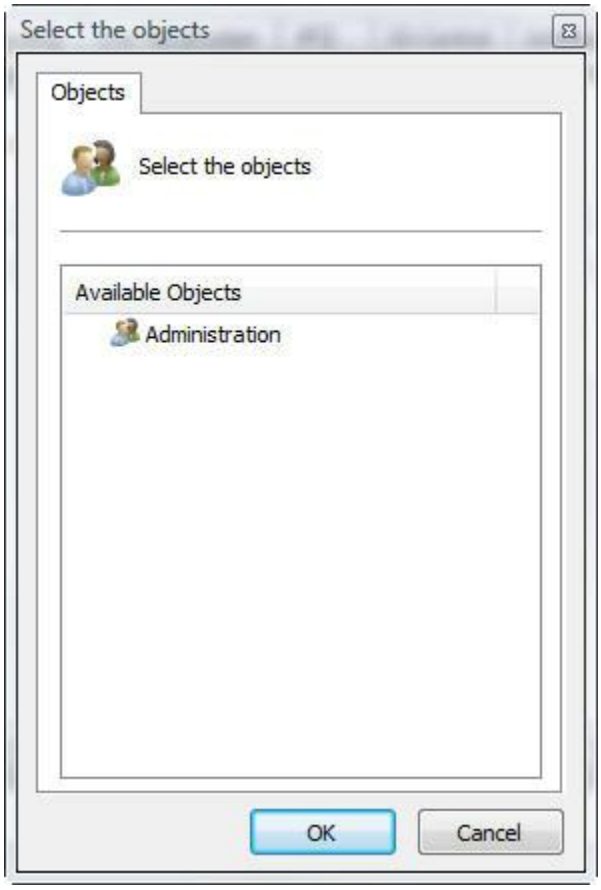
© 2002 - 2011 by Optiview USA all rights



This screen presents two lists, one of groups and the other of users, the list of available groups, located at the left, and the list of allowed users, located at the right.

To give the right of viewing to a group, simply click on Add Groups and choose the desired group in the screen shown in Figure bellow:

© 2002 - 2011 by Optiview USA all rights



This rights are duplicated in the Surveillance Client in the Recordings area. Only the cameras that the user has logged have the right to view to view recordings will appear in the list of cameras.

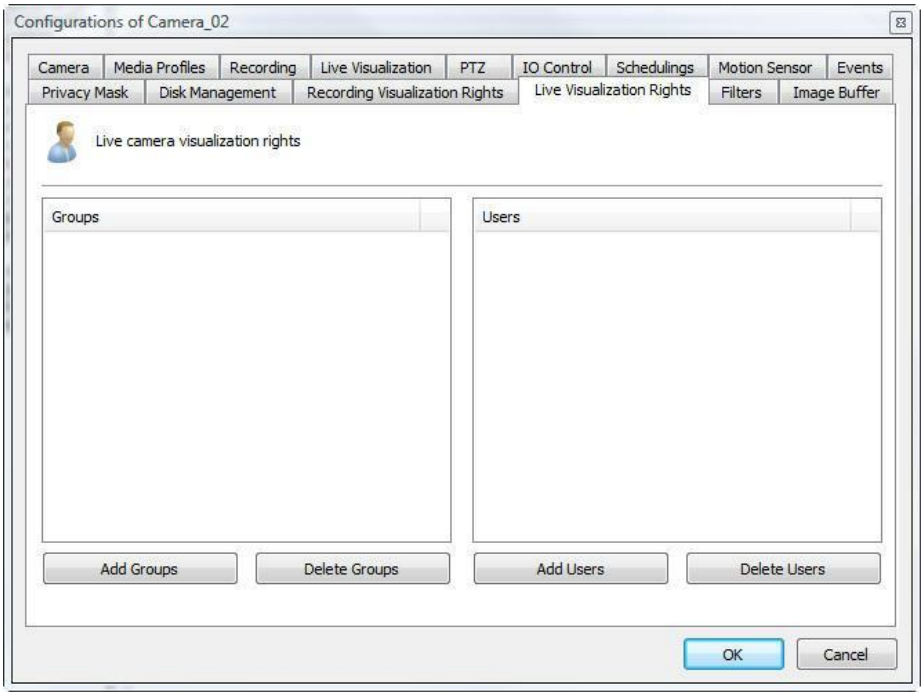
6.1.10 How to configure the live visualization rights

The area of definition of live visualization rights works in a similar way to that of the recording visualization rights, except that in this area is defined which users will have access to visualization of the camera in real time. Reading of the previous topic is advisable for a better assimilation of the concept.

These rights are mirrored in the Surveillance Client where only those cameras to which access was granted are shown to the user.

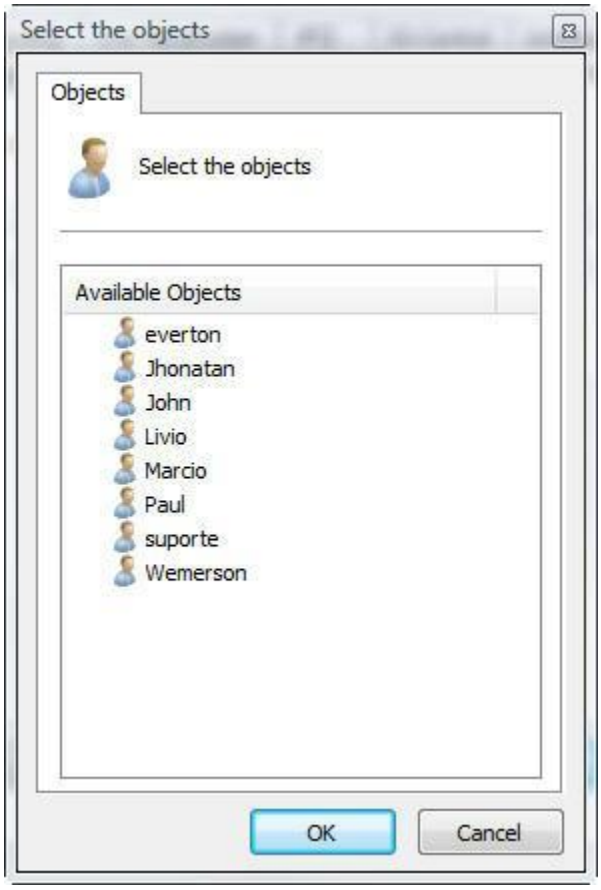
To access this feature, click on the Live **Visualization Rights** tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



To give the right of viewing of recordings to the desired users/groups, simply click on **Add Groups/Users** and select them from the list of **Groups/Users** which will come up as shown in Figure bellow:

© 2002 - 2011 by Optiview USA all rights



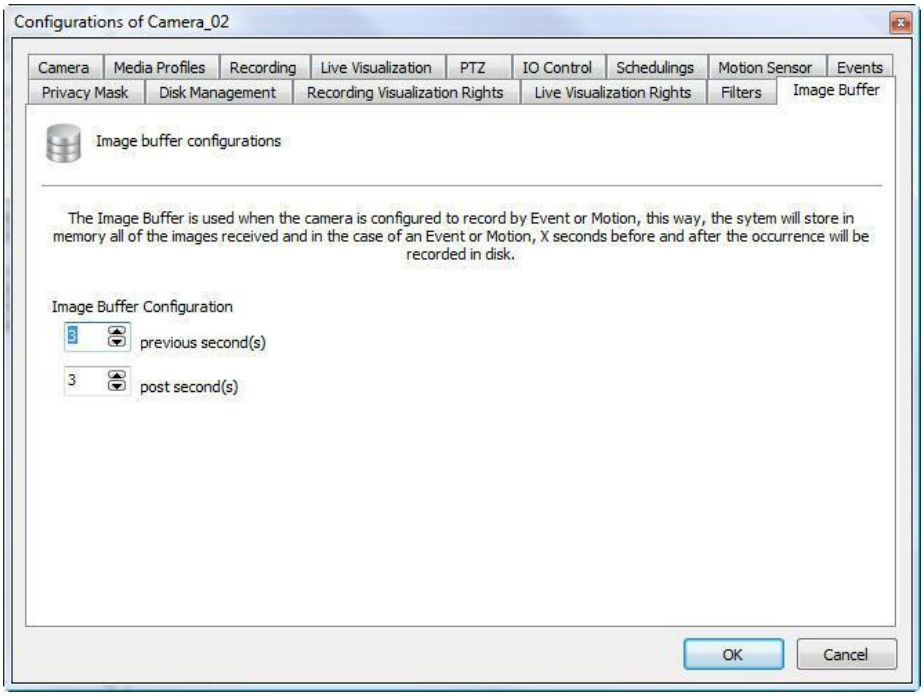
Select the available user and click on **OK**. The same rule applies to the list of groups.

6.1.11 How to configure the Image Buffer

The Image Buffer is used when the camera is configured to record by motion detection. This way, the system stores the receive images in memory, and in case of motion detection, X seconds prior to and after the motion are also recorded in disk. To learn how to do the configuration of motion recording see How to configure the Motion Sensor.

To access this feature, click on the Image Buffer tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



By default, the initial value of this configuration is three seconds before and three seconds after. The greater the number of configured seconds, the more processing used by Digifort for the storage of the images.

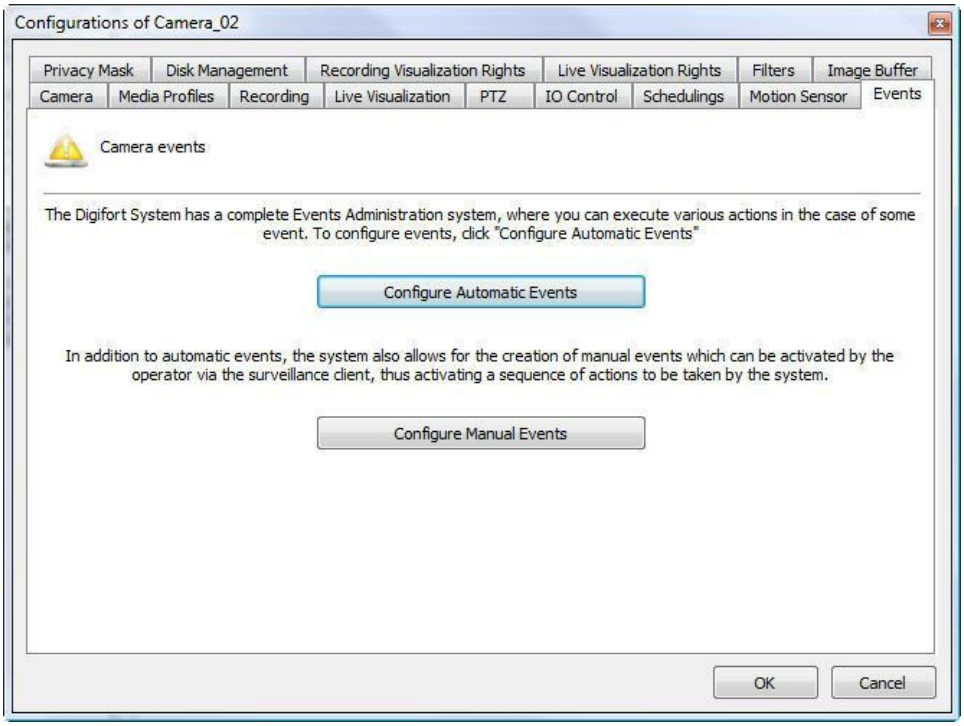
6.1.12 How to configure camera events

During the operation of the camera in the Digifort System, various events occur in the camera. These events can be communication failures or alarm recognition events, for example.
By configuring the events of the camera, it's possible to specify a set of actions that Digifort will undertake when a determined event occurs.

Digifort Enterprise offers control over automatic events, that is, events that occur without user intervention, and manual events, which are events generated based on intervention of the user.

To access this feature, click on the **Events** tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights


Configurations of Camera_02
Privacy Mask
Disk Management
Recording Visualization Rights
Live Visualization Rights
Filters
Image Buffer
Camera
Media Profiles
Recording
Live Visualization
PTZ
IO Control
Schedulings
Motion Sensor
Events
Camera events
The Digifort System has a complete Events Administration system, where you can execute various actions in the case of some event. To configure events, click "Configure Automatic Events"
Configure Automatic Events
In addition to automatic events, the system also allows for the creation of manual events which can be activated by the operator via the surveillance client, thus activating a sequence of actions to be taken by the system.
Configure Manual Events
OK
Cancel

6.1.12.1 How to configure automatic events

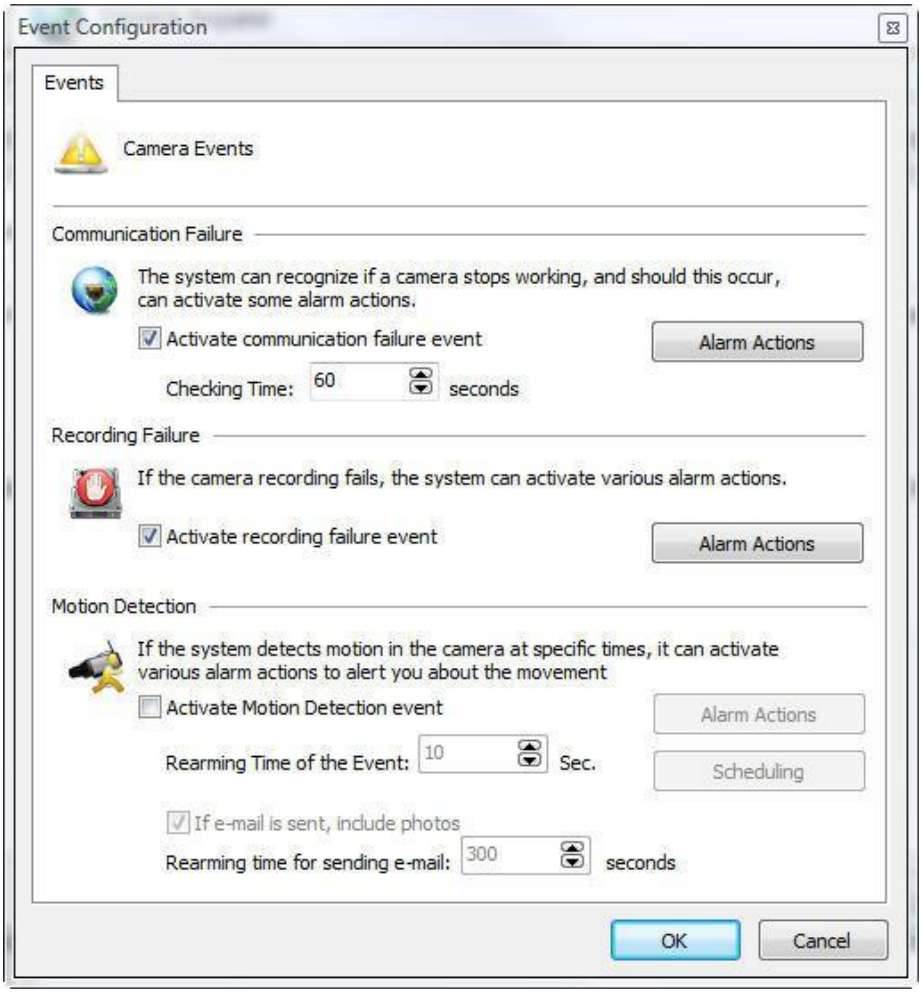
Digifort Enterprise offers control over automatic events, which are: failure of communication with the camera, failure of recording images in disk, and motion detection in the camera.

The communication failures occurs when a camera looses contact with the server, which could be sign of violence against the camera (attack on site with destruction of the equipment), or could be sign of mishap (fire), lack of electrical power, or even abnormalities in the system. The recording failures occur when the server's disk burns, for example, and motion detection occurs when some motion in the scene is detected by the camera.

For all events, it's possible to define a different set of alarm actions, by simply clicking on the corresponding **Alarm Actions** button.

To configure the automatic events, click on Configure Automatic Events, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights


Event Configuration
Events
Camera Events
Communication Failure
The system can recognize if a camera stops working, and should this occur, can activate some alarm actions.
Activate communication failure event
Alarm Actions
Checking Time: 60 seconds
Recording Failure
If the camera recording fails, the system can activate various alarm actions.
Activate recording failure event
Alarm Actions
Motion Detection
If the system detects motion in the camera at specific times, it can activate various alarm actions to alert you about the movement
Activate Motion Detection event
Alarm Actions
Rearming Time of the Event: 10 Sec.
Scheduling
If e-mail is sent, include photos
Rearming time for sending e-mail: 300 seconds
OK
Cancel

6.1.12.1.1 How to configure the communications failure event

To configure the communications failure event, mark the option **Activate** communications failure event and specify the failure checking time. With this value informed, every X seconds the alarm actions will occurs again until the problem is solved.

To learn how to configure the alarm actions, see How to configure the alarm actions

6.1.12.1.2 How to configure the recording failure event

To configure the communications failure event, mark the option Activate recording failure event.

To learn how to configure the alarm actions, see How to configure the alarm actions

© 2002 - 2011 by Optiview USA all rights

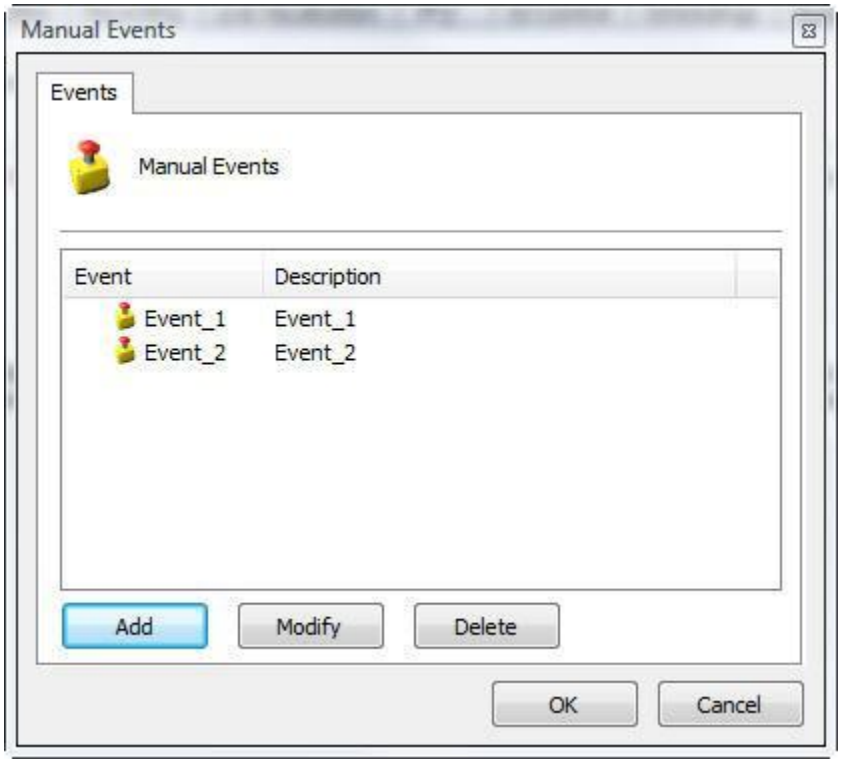
6.1.12.1.3 How to configure the motion detection event

To configure the communications failure event, mark the option Activate motion detection event.
The configuration of this event involves the following parameters:

- **Activate motion detection event**: Activates the motion detection event.
- **Rearming time of the event**: Specify the value in seconds in which Digifort will recognize new motions after a motion has occurs.
- **If sending e-mail, include photos**: Include the photo in which there was motion if sending notification e-mail.
- **Rearming time of the sending of e-mail**: Specify the time interval in which Digifort will send another e-mail message in case the motion event still is recognized.
- **Alarm Actions button:** Click on this button to define the actions that Digifort will execute when the event of motion detection was detected. To learn how to configure the alarm actions, see How to configure the alarm actions
- **Scheduling**: Click on this button to define the times of days and days of the week in which Digifort is to recognize motion events. If this configuration is not done, the motion events will be recognized 24 hours per day and 7 days per week. To learn how to configure the scheduling, see How to configure the scheduling of recording

6.1.12.2 How to configure the manual events

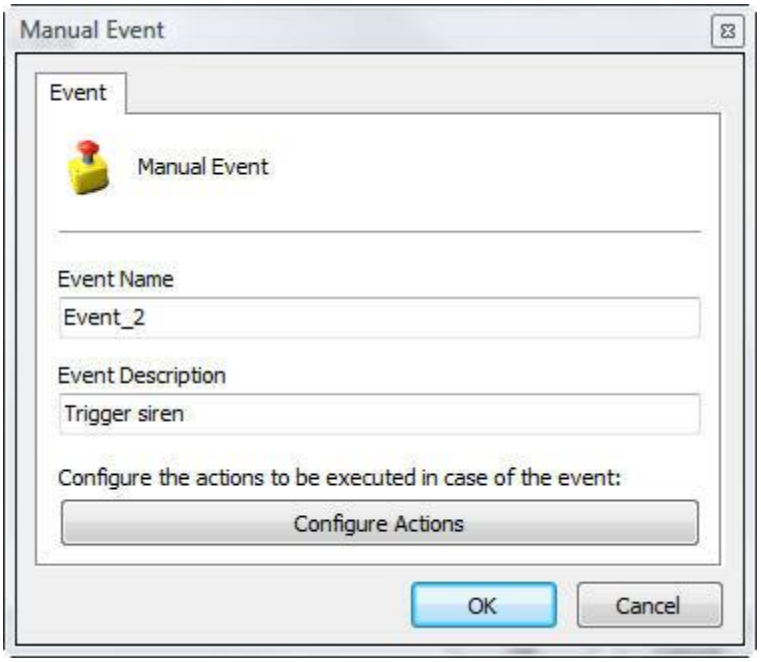
To configure the manual events, click on Configure Manual Events, as shown in the picture below:



© 2002 - 2011 by Optiview USA all rights

In this screen, you must register the manual events that can be activated by the operator in the Surveillance Client. In the example of the picture above there is an event registered that opens a door.

To learn how to activate manual events by way of the Surveillance Client, consult its manual.
To add a manual event, click on the Add button, opening the screen below. To modify and exclude, click on the corresponding button.

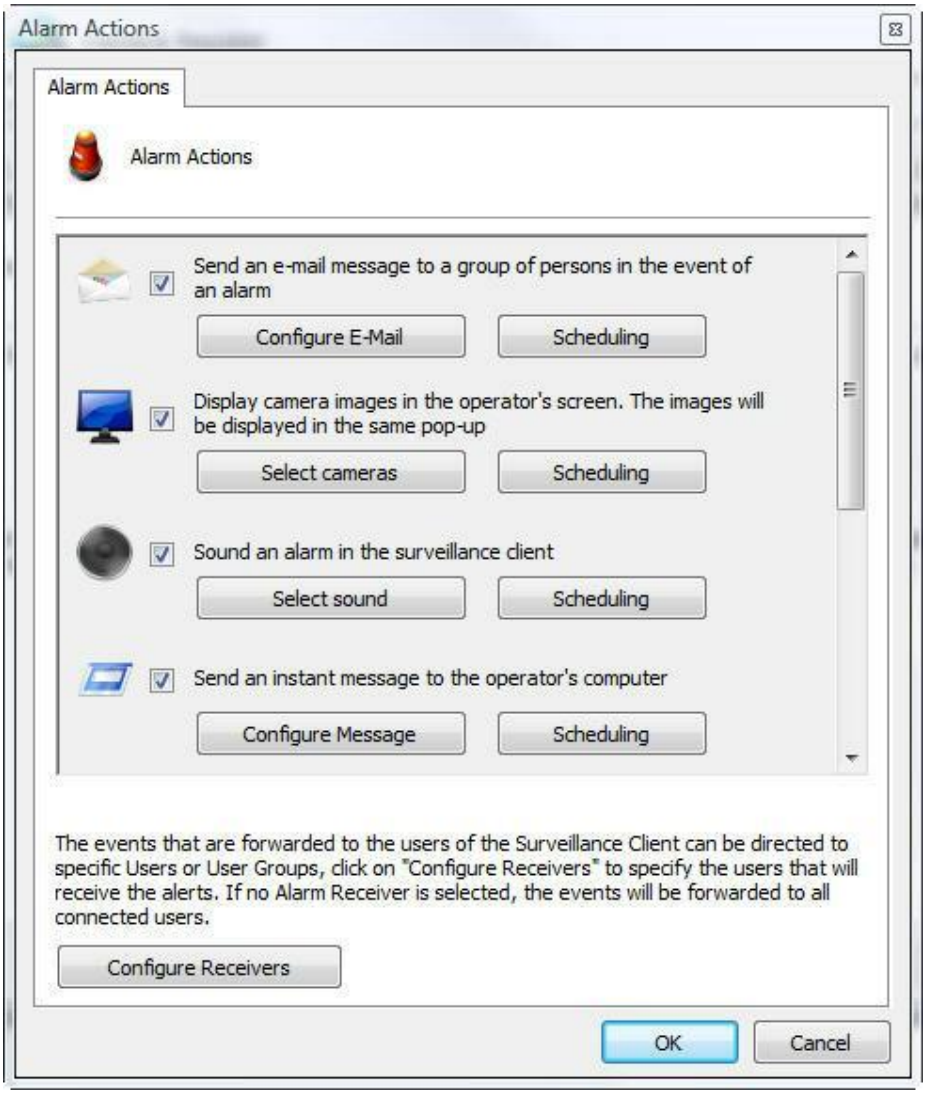


Enter the name and a description of the event in this screen and then click on Configure Actions. To learn how to configure the actions that this manual event will execute, see How to configure the alarm actions

6.1.12.3 How to configure the alarm actions

Various events require the configuration of alarm actions. To access these configurations, click on the Alarm Actions corresponding to the executed configuration. After clicking on this button the screen of alarms configuration will be displayed, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights

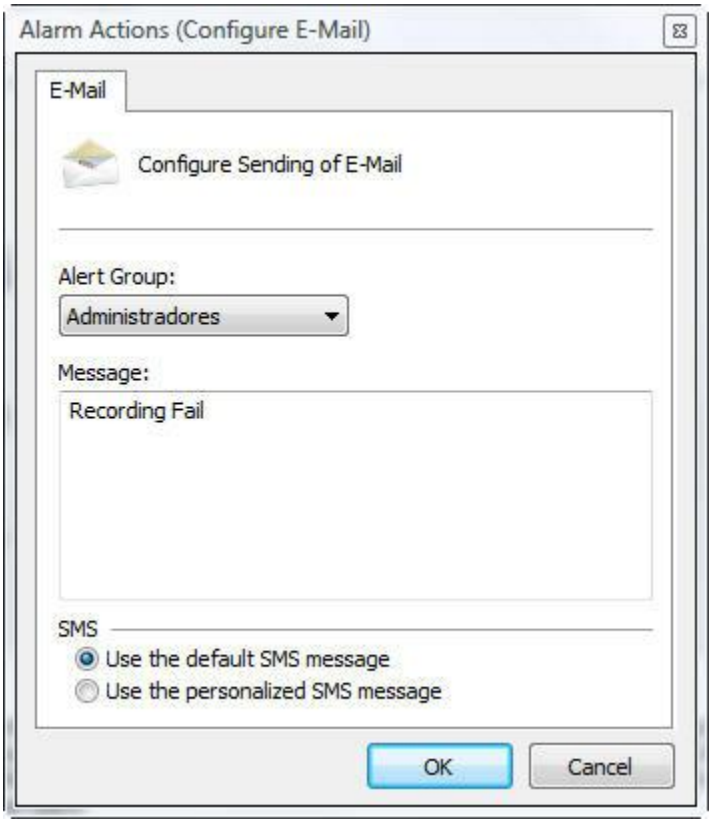

Alarm Actions
Alarm Actions
Alarm Actions
Send an e-mail message to a group of persons in the event of an alarm
Configure E-Mail
Scheduling
Display camera images in the operator's screen. The images will be displayed in the same pop-up
Select cameras
Scheduling
Sound an alarm in the surveillance client
Select sound
Scheduling
Send an instant message to the operator's computer
Configure Message
Scheduling
The events that are forwarded to the users of the Surveillance Client can be directed to specific Users or User Groups, click on "Configure Receivers" to specify the users that will receive the alerts. If no Alarm Receiver is selected, the events will be forwarded to all connected users.
Configure Receivers
OK
Cancel

Digifort Enterprise offers eight alarm actions. Each alarm action has its own individual scheduling so that you can configure in which hours and days of the week the events can occurs.

6.1.12.3.1 Send an e-mail message to a group of persons in the case of an alarm

Sends notification e-mail to a selected alert group. If you wish to execute this action in case of the selected event, mark this option and click on Configure E-mail, opening the configuration screen of the e-mail message to be sent, as shown in picture below:

© 2002 - 2011 by Optiview USA all rights

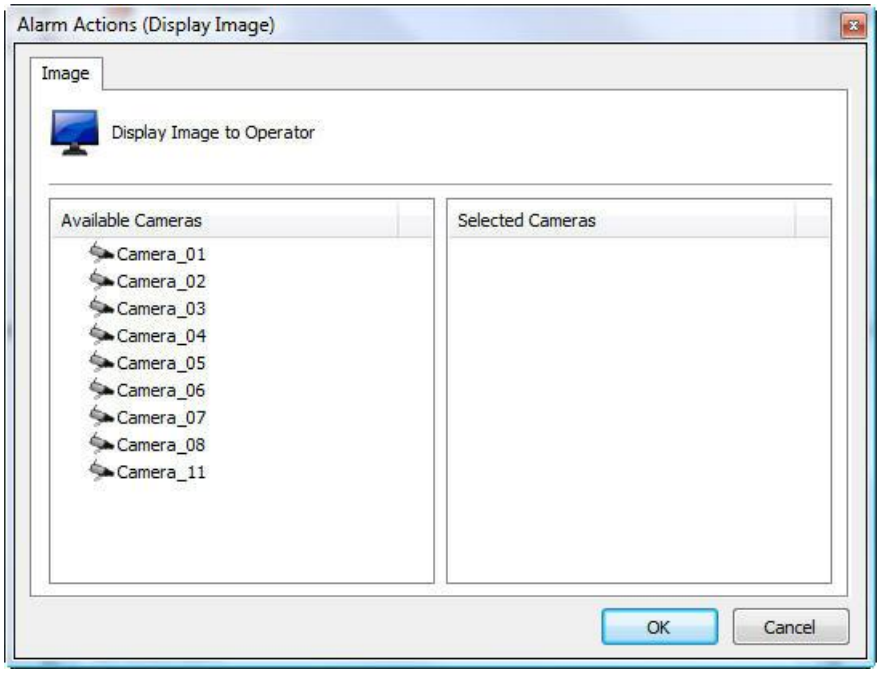


In this screen, select the alert group that will receive the e-mail and the message that will be sent to the group.

6.1.12.3.2 Display camera images in the screen of the operator

Displays images from any camera of the system in the screen of the operator of the Surveillance Client in a pop-up. The number of cameras that can be displayed in a pop-up is unlimited, that is if more than one camera is selected, an automatic view will be created. To learn about surveillance views, see the manual of the Surveillance Client. If you wish to execute this action in case of the selected event, mark this option and click on Select Cameras, opening the configuration screen of cameras to be displayed on the screen, as shown in picture below:

© 2002 - 2011 by Optiview USA all rights



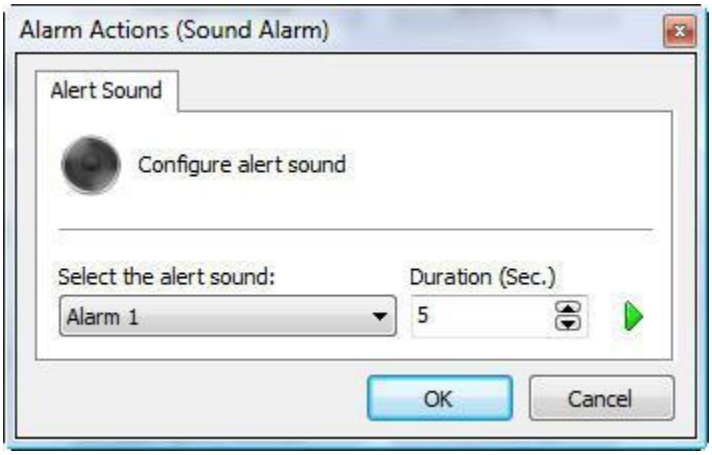
To select the cameras to be displayed on the operator's screen, select the desired cameras in the list of available cameras and drag them to the list of selected cameras.

To remove the cameras to be displayed on the operator's screen, select the desired cameras in the list of selected and drag them to the list of available cameras.

6.1.12.3.3 Sound an alarm in the Surveillance Client

Sounds an alarm in the Surveillance Client, alerting the operator to the event that occurred. If you wish to execute this action, in case of the selected event, mark this option and click on Select Sound, opening the configuration screen of the sound to be executed in the Surveillance Client, as shown in picture below:

© 2002 - 2011 by Optiview USA all rights



Select the desired alert sound and execution time in the Surveillance Client. To test the selected sound, click on the **Play** button.

6.1.12.3.4 Send instant message to the operator of the computer

Send an instant message to the operator with information defined by the administrator. These messages can contain instructions of the procedure to be executed by the operator for solution of the problem, for example. If you wish to execute this action in case of the selected event, mark this option and click on Configure Message, opening the configuration screen of the message to be displayed on the Surveillance Client, as shown in picture below:

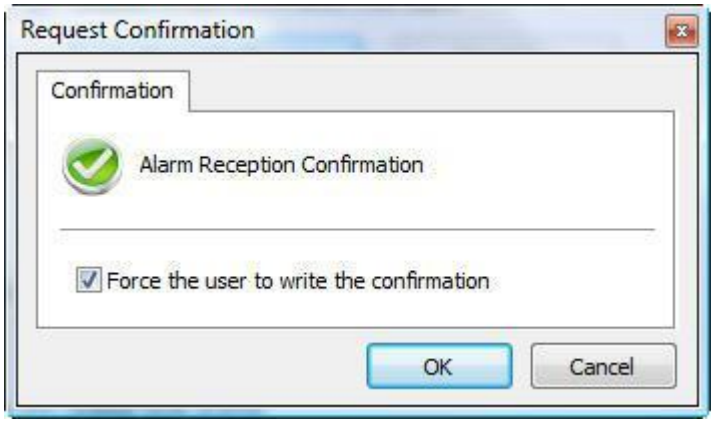


In this screen, configure the message to be displayed to the operator on the Surveillance Client.

© 2002 - 2011 by Optiview USA all rights

6.1.12.3.5 Request written confirmation from users

Requests a written confirmation from the users. This confirmation will be displayed to the operator in the Surveillance Client. These confirmations can contain information about the procedure that the operator executed in the case of an event. If you wish to execute this action in case of the selected event, mark this option and click on Configure Confirmation, opening the screen for configuration of the confirmation to be displayed on the Surveillance Client, as shown in picture below:

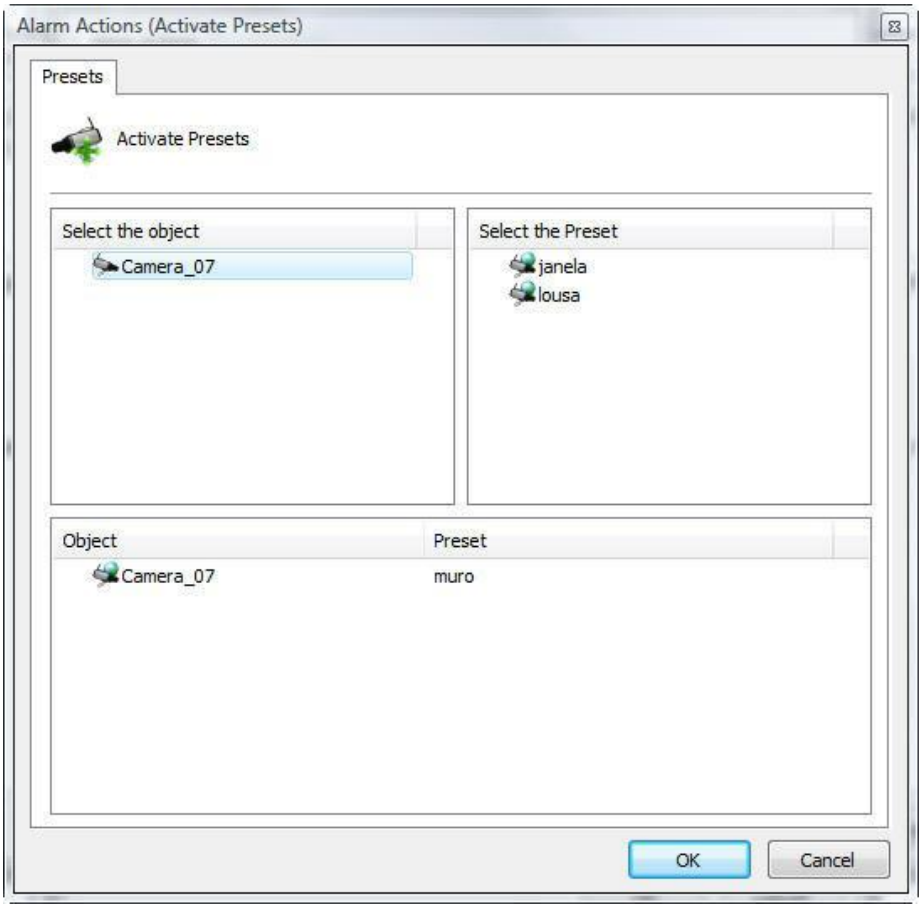


If you wish to oblige the operator to write a confirmation, mark this option..

6.1.12.3.6 Activate camera presets

Activates camera presets when an event occurs, that is, when this event occurs, some cameras can be configured to position themselves in a pre-defined position. To learn how make presets see How to configure the Presets Controls.If you wish to execute this action in case of the selected event, mark this option and click on Configure Presets, as shown in picture below:

© 2002 - 2011 by Optiview USA all rights

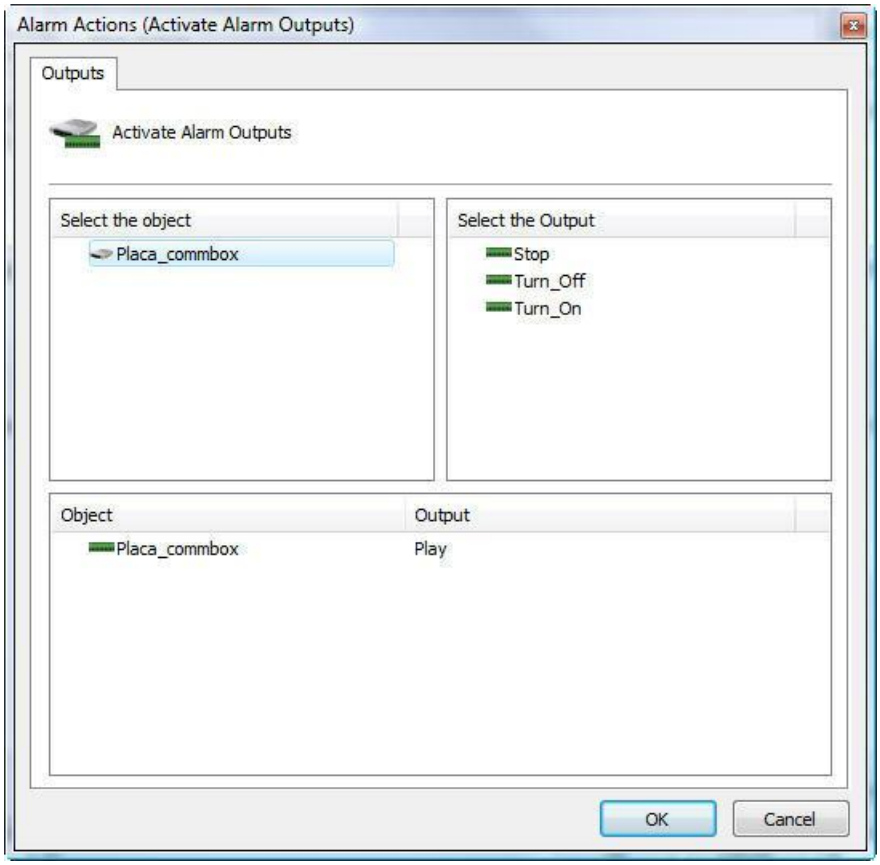


In this screen, select the desired camera, select the preset that you wish to activate, and then drag it to the list below, as shown in the picture below:

6.1.12.3.7 Activate action scripts of alarm outputs

When an event occurs, this option lets Digifort activate action scripts of alarm outputs, such as, for example, setting off a siren. To learn how to configure scripts of alarm outputs, see How to add output events. If you wish to execute this action in the case of the selected event, mark this option and click on Configure Actions, as shown in picture below:

© 2002 - 2011 by Optiview USA all rights



In this screen, select the camera or alarm device which contains the script of actions of the alarm output that you want to activate. Following this, select the event and drag it to the list below, as shown in the picture below:

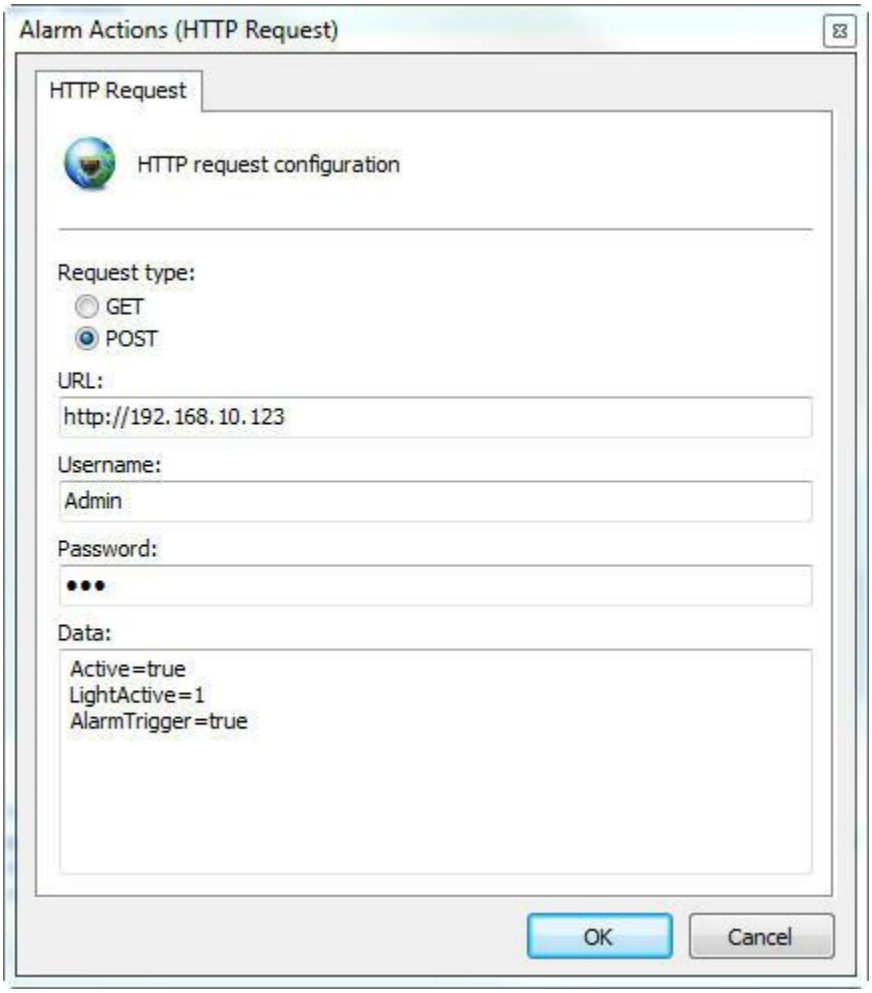
6.1.12.3.8 Send a HTTP Request

The HTTP request aims to create a channel of communication between Digifort and external software. This action allows integration of Digifort with any hardware or software that can process HTTP commands, for example: cameras, access control software, etc.

This feature requires a minimum knowledge of web programming for better understanding of its operation.

To start setup click "**Configure request".** And the following screen appears:

© 2002 - 2011 by Optiview USA all rights



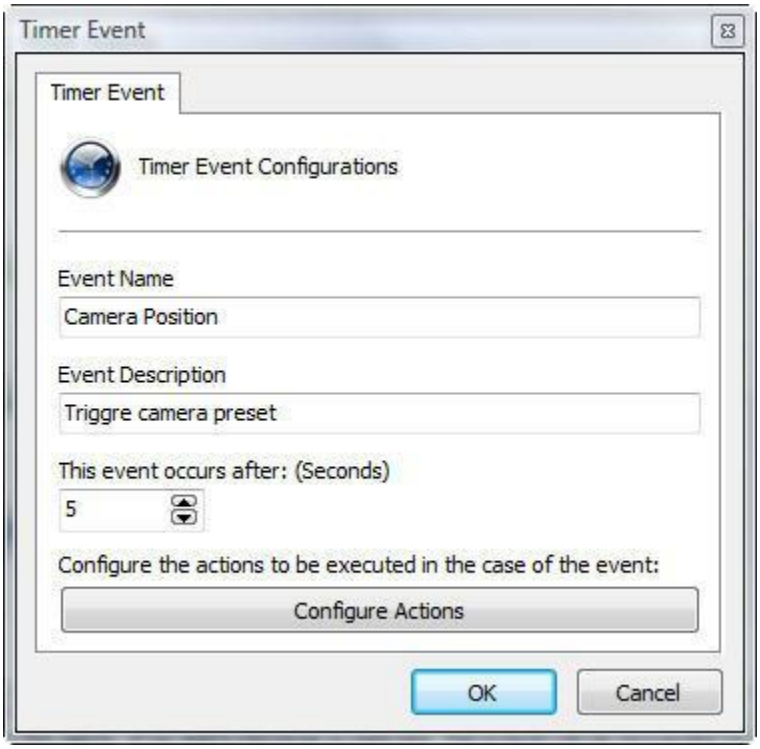
This screen has the following settings:

- **Request type**: Request: GET, where all parameters are in the URL.
- **Username:** User authentication command.
- **Password:** password for authentication command.
- **Data:** when the request: POST is selected the field for data becomes available.

6.1.12.3.9 Create timer events

Timer events are events that set off other configured time events. They can be, for example, upon recognizing motion in some camera: set off a siren at the exact moment of the event, and via timer event, position a camera in a determined position five seconds later. If you wish to execute this action in case of the selected event, mark this option and click on **Configure Actions**, as shown in picture below:

© 2002 - 2011 by Optiview USA all rights



In this screen, enter the name of the event, its description, and define how many seconds after the main event that it will happen. Lastly, click on Configure Actions to configure the actions that this event will execute. To learn how to configure alarm actions, see How to configure the alarm actions.

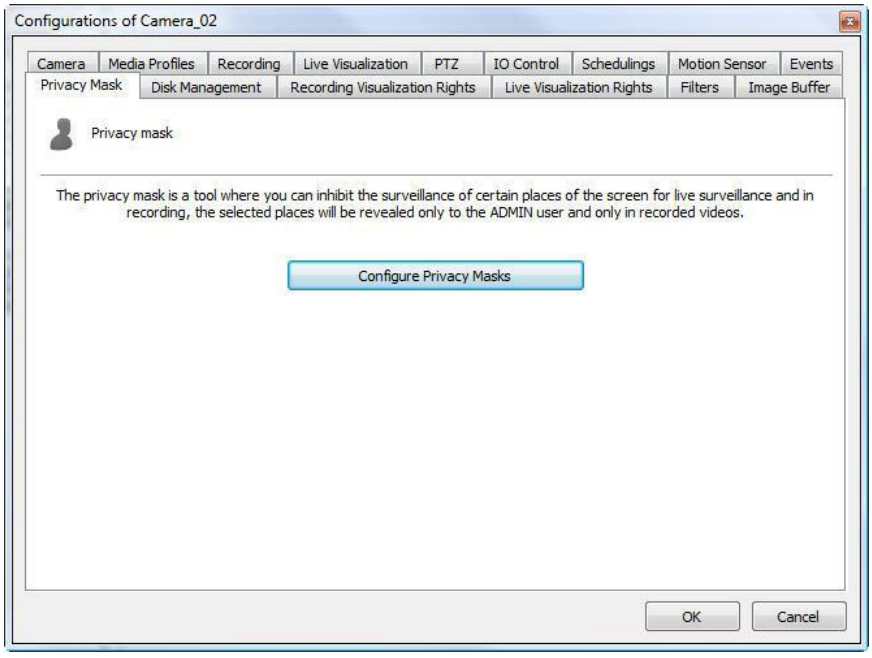
6.1.13 How to configure the Privacy Mask

The privacy mask is a tool which makes it possible to occult areas of the image that can't be observed by the operator.

It's important to emphasize that the privacy mask is not written in the server, but to the contrary, the original image is recorded and when the image is displayed on the screen, the privacy mask is applied.

The privacy mask is not applied in the admin user, as he has all system access rights.
To access this feature, click on the **Privacy Mask** tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



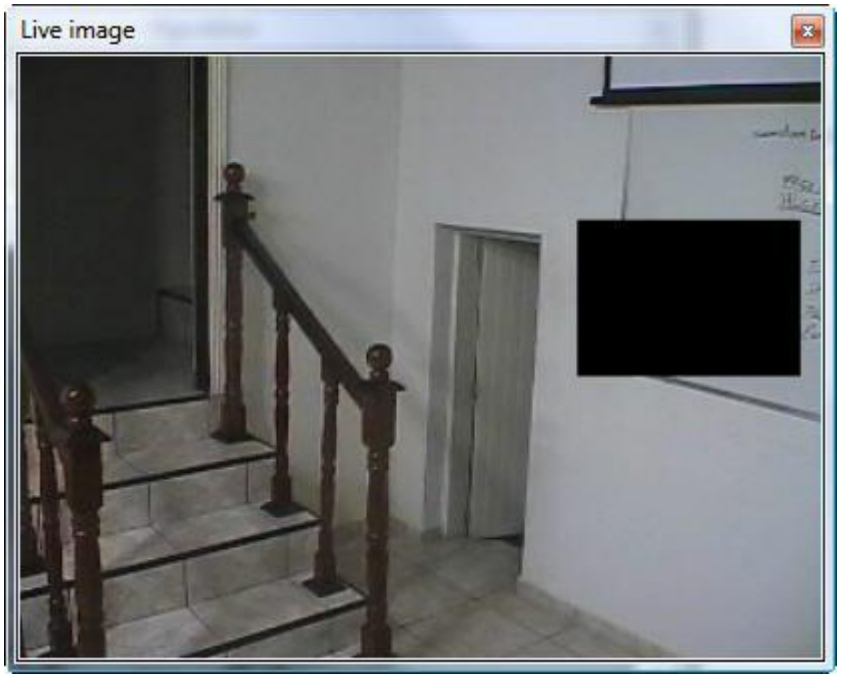
To configure the privacy mask, click on Configure Privacy Masks, as shown in the picture below:



© 2002 - 2011 by Optiview USA all rights

In the example of the picture above the visualization of the entrance of the house is not permitted to the operator. The effect of this configuration is demonstrated in the picture below:

To add a privacy mask, click on the left button of the mouse over the image and drag it, forming a rectangle. To remove a selected area, make a rectangle with the right button of the mouse englobing all of the area of the mask to be removed, or click on **Eliminate Selection** to eliminate all of the created masks.



6.1.14 How to configure the Disk Management

Digifort has an advanced system of disk management, responsible for the administration of the recorded images.

For good performance of the server, this configuration must be very well thought out before executing, as it involves several factors such as available disk space, type of recording selected for the camera, number of cameras in the system, etc.

As the space we have in disk is always limited, Digifort needs to eliminate old recordings to store new ones. For this purpose, a time limit or space limit for the recordings must be specified, so that when the configured limit is reached, the old recordings are eliminated, freeing space for the new recordings.

The disk manager offers three types of configurations, these being: recording by limit of days, recording by limit of hours and recording by limit of disk space.

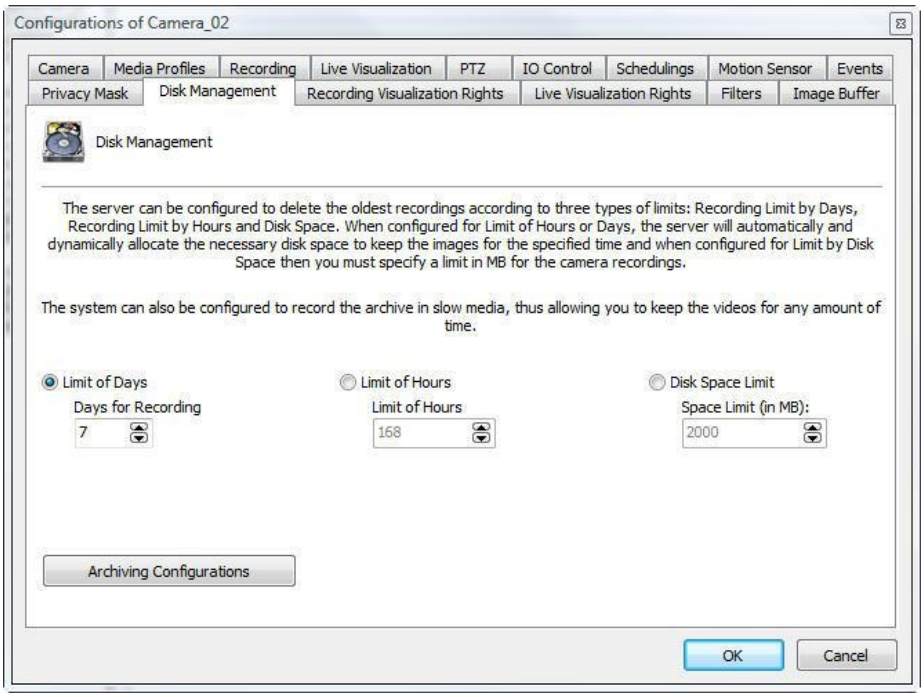
The disk manager includes three types of configurations: recording by day limit; recording by time limit; and recording by disk space limit.

© 2002 - 2011 by Optiview USA all rights

In the types of configuration by day and time limits, the system automatically allocates the space needed to record the images within the limit specified by making a statistical analysis based on the images already recorded by the camera. A set of cameras that does not need much space will then transfer that unused space to another camera that needs it, always respecting the recording limit configured for each camera. With Digifort you can record images in various storage places and HDs (for example: RAID5 or superior) automatically counterbalancing the amount of recording.
This is the most recommended method and the most reliable one guaranteeing that the images will be found in the future when requested if the day limit has not been surpassed.

In recording by disk space limit, the quantity of disk space to be used by the camera must be specified.

When this limit is surpassed, the system automatically eliminates the oldest recordings of the camera, in order to occupy only the configured space.
To access this feature, click on the Disk Management tab, as shown in the picture below:


Configurations of Camera_02
Camera
Media Profiles
Recording
Live Visualization
PTZ
IO Control
Schedulings
Motion Sensor
Events
Privacy Mask
Disk Management
Recording Visualization Rights
Live Visualization Rights
Filters
Image Buffer
Disk Management
The server can be configured to delete the oldest recordings according to three types of limits: Recording Limit by Days, Recording Limit by Hours and Disk Space. When configured for Limit of Hours or Days, the server will automatically and dynamically allocate the necessary disk space to keep the images for the specified time and when configured for Limit by Disk Space then you must specify a limit in MB for the camera recordings.
The system can also be configured to record the archive in slow media, thus allowing you to keep the videos for any amount of time.
Limit of Days
Days for Recording
7
Limit of Hours
Limit of Hours
168
Disk Space Limit
Space Limit (in MB):
2000
Archiving Configurations
OK
Cancel

6.1.14.1 Recording by limit of days

Recording by limit of days keeps the camera images stored in disk during only the specified absolute number of days.
For a better understanding of this type of configuration, let's suppose we have these two situations:

1. The recording mode of the camera is configured for continuous recording (always record) and the limit of days of recording is configured for

© 2002 - 2011 by Optiview USA all rights

seven days. With this configuration, seven days of images are stored in disk, and when the eighth day comes, the oldest recording (first day) will be deleted.

2. The recording mode of the camera is configured for recording by motion detection and the limit of days of recording is configured for seven days. Supposing that, of these seven days, only four had motion, then only four days of images are stored in disk, and when the eighth day comes, the oldest recording will be deleted.

As we can observe by the situations described, we must be very careful with this configuration, since if the camera is recording by motion detection, it's not always recording in disk the specified number of days, since there was no motion on some days, the images of these days are not recorded. This is due to the fact that the configured number of consecutive days will be recorded. configurados.

6.1.14.2 Recording by limit of hours

Recording by limit of hours keeps the camera images stored in disk during only the specified absolute number of days.
For a better understanding of this type of configuration, let's suppose we have these two situations:

1. The recording mode of the camera is configured for continuous recording (always record) and the limit of hours of recording is configured for 168 hours. With this configuration, the last 168 hours of images are stored in disk, the equivalent of exactly seven days. When the 169th hour comes, the system will eliminate the limit configured in days, freeing disk space for new recordings.

2. The recording mode of the camera is configured for recording by motion detection and the limit of hours of recording is configured for 168 hours. Supposing that in the last two days there was no motion detection in this camera. Then the equivalent of nine days will be stored in disk, even though 168 hours is equivalent to seven days. When the 169th hour comes, the system will eliminate the limit configured in days, freeing disk space for new recordings.

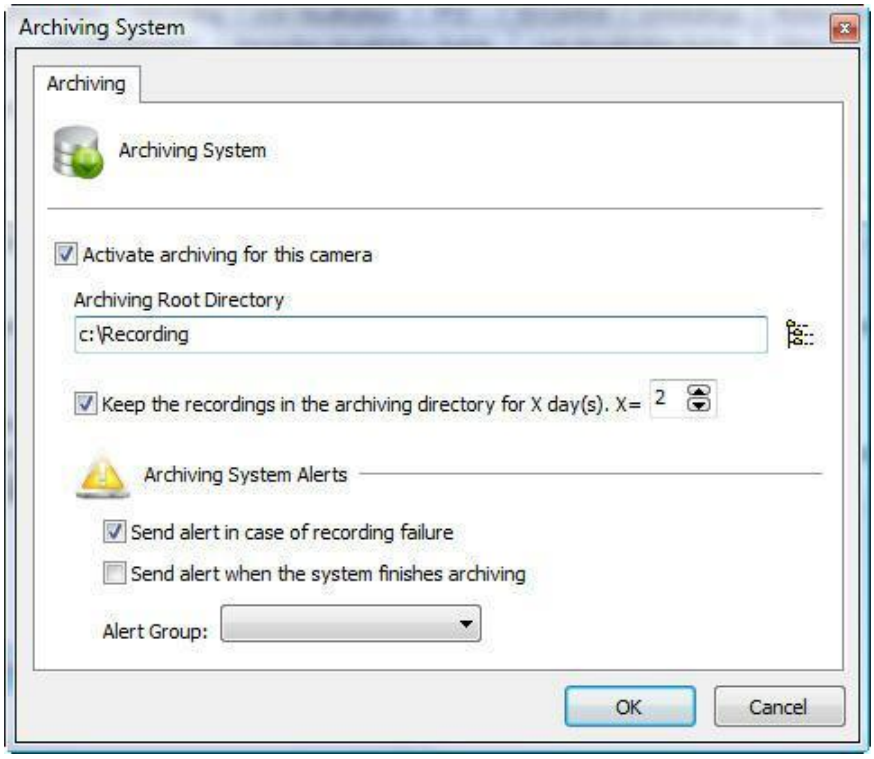
Tip: Using the limit of recording by hours in a very interesting alternative, when used together with motion detection, as it maximizes the number of hours that can be recorded in disk.

6.1.14.3 How to configure the archiving

Digifort makes it possible for the recordings of a camera to be sent to a different disk or computer in the network, aimed at executing backups in tape or other backup device.
In this configuration, the number of days in which the recordings must be kept in disk or the specified computer of the network can be specified.

To access this feature, click on **Configurations of Archiving**, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



- **Activate the archiving for this camera**: Activates the archiving for the camera being edited.
- **Root Directory of archiving**: Enter the directory in which the archiving will be done.
- **Keep the recordings in the archiving directory for X days**: Enter the number of days the images of the cameras shall be maintained. Exactly the specified last X days will be kept. Previous days will be eliminated.
- **Send alert in case of recording failure**: If some error occurs during the archiving, an e-mail notification can be sent. For this purpose, mark this option and select the desired alert group.
- **Send alert when the system finishes the archiving**: Sends an e-mail notification to the selected alert group when the archiving is successfully completed.

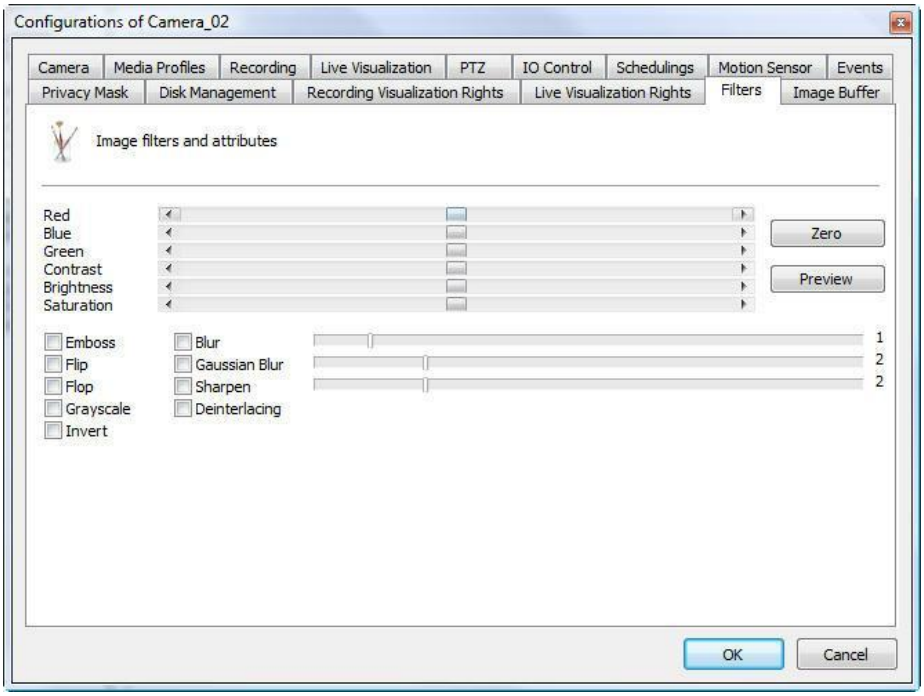
6.1.15 How to configure the image effects

Digifort is equipped with a set of effects that can be applied to the image so that cameras that have an impaired image can be improved.

This set of effects is only applied during the camera's visualization in the Surveillance Client, that is, the camera's original image is stored in the server.

To access this feature, click on the Effects tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights

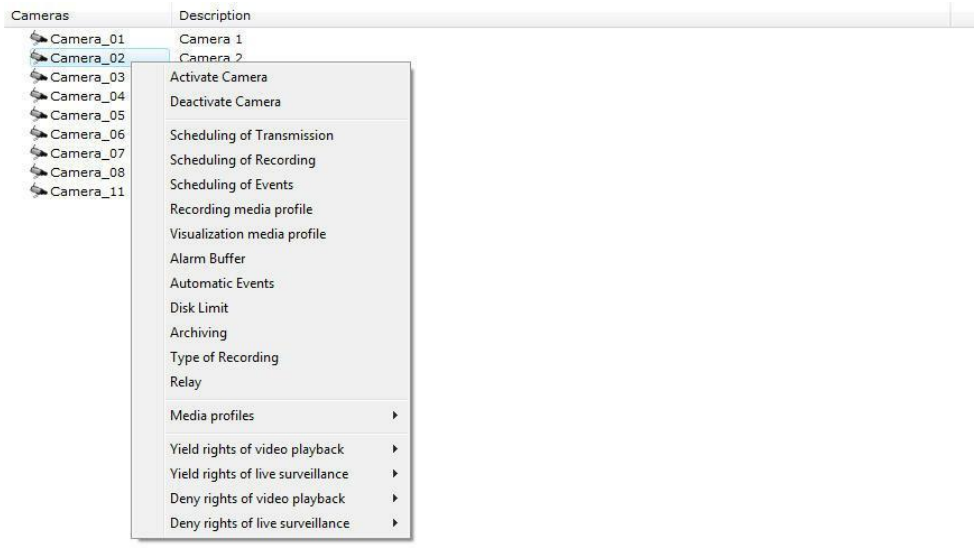


- **Red**: Adjusts the level of the color red in the image.
- **Blue**: Adjusts the level of the color blue in the image.
- **Green**: Adjusts the level of the color green in the image.
- **Contrast**: Adjusts the level of contrast in the image.
- **Brightness**: Adjusts the level of brightness in the image.
- **Color level**: Adjusts the level of color in the image.
- **Zero button**: Returns the above mentioned values to their initial positions.
- **Preview button**: Opens the video of the camera with the applied configurations.
- **Emboss**: Leaves the image in gray tones to highlight relief.
- **Flip**: Inverts the image horizontally. Recommended when the camera is installed in an inverted position.
- **Flop**: Inverts the image vertically. Recommended when the camera is installed in an inverted position.
- **Grayscale**: Leaves the image in gray tones.
- **Blur**: Applies a blurring effect to the image. Adjust the intensity level of the filter using the slide bar alongside.
- **Gaussian Blur**: Applies a Gaussian blurring effect to the image. Adjust the intensity level of the filter using the slide bar alongside.
- **Sharpen**: Applies a border highlight effect to the image.

6.1.16 Camera management functions

Digifort allows the basic configurations in common with all cameras to be applied in batch.
Select the desired cameras and click on the right button, opening the Options Menu, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



The options menu offers the following functions:

6.1.16.1 Activate camera

Activates the recording of the selected cameras

6.1.16.2 Disactivate camera

Disactivates the recording of the selected cameras

6.1.16.3 Transmission scheduling

Configures the scheduling of transmission of the selected cameras. To learn how to use this feature, see How to configure the scheduling of transmission

6.1.16.4 Recording scheduling

Configures the scheduling of recording of the selected cameras. To learn how to use this feature, see How to configure the scheduling of recording.

6.1.16.5 Events scheduling

Configures the scheduling of events of the selected cameras. To learn how to use this feature, see How to configure the scheduling of recording.

© 2002 - 2011 by Optiview USA all rights

6.1.16.6 Media Profiles

Add, Alter or Exclude the Media Profiles for several cameras simultaneously, as long as they have the same media options. To select the cameras with the same media profile, select a desired camera and press Ctrl + M. If there are cameras with the same media profile as the selected camera, it will automatically be selected.

6.1.16.7 Recording media profile

Simultaneously configure the type of profile of the recording media for the cameras with the same profile as the configuration. To select the cameras with the same media profile, select a desired camera and press Ctrl + M. If there are cameras with the same media profile as the selected camera, it will automatically be selected.

6.1.16.8 Viewing media profile

Simultaneously configure the type of profile of the viewing for the cameras with the same profile as the configuration. To select the cameras with the same media profile, select a desired camera and press Ctrl + M. If there are cameras with the same media profile as the selected camera, it will automatically be selected.

6.1.16.9 Alarm buffer

Modifies the configurations of the image buffer. To learn how to use this feature, see How to configure the Image Buffer.

6.1.16.10 Automatic events

Configures the automatic events of the selected cameras. To learn how to use this feature, see How to configure automatic events

6.1.16.11 Disk limit

Modifies the configurations of the disk limit of the selected cameras. To learn how to use this feature, see Disk Limits

6.1.16.12 Type of recording

Modifies the type of recording of the selected cameras. To learn how to use this feature, see How to configure the recording of the camera

6.1.16.13 Relay

Activate Relay for the selected cameras. To learn how to config this feature see How to configure the visualization of the camera

© 2002 - 2011 by Optiview USA all rights

6.1.16.14 Give video playback rights

Give video playback rights: To give viewing rights for video playback to selected cameras. In the option users or groups, a screen will open up with a list of all users or groups registered in the system. Select the users/ gruops to whom you want to give the right to video playback for these cameras and click on OK. To lear more about video playback rights see Users rights

6.1.16.15 Give live surveillance rights

To give viewing rights for live surveillance to selected cameras. In the option users or groups, a screen will open up with a list of all users or groups registered in the system. Select the users/gruops to whom you want to give the right to video playback for these cameras and click on OK. To learn more about surveillance rights see Users rights

6.1.16.16 Deny video playback rights

Denies video playback rights for the selected cameras. In the option users or groups, a screen will open up with a list of all users or groups registered in the system. Select the users/gruops to whom you want to give the right to video playback for these cameras and click on **OK**. To learn about video playback rights see Users rights

6.1.16.17 Deny live surveillance rights

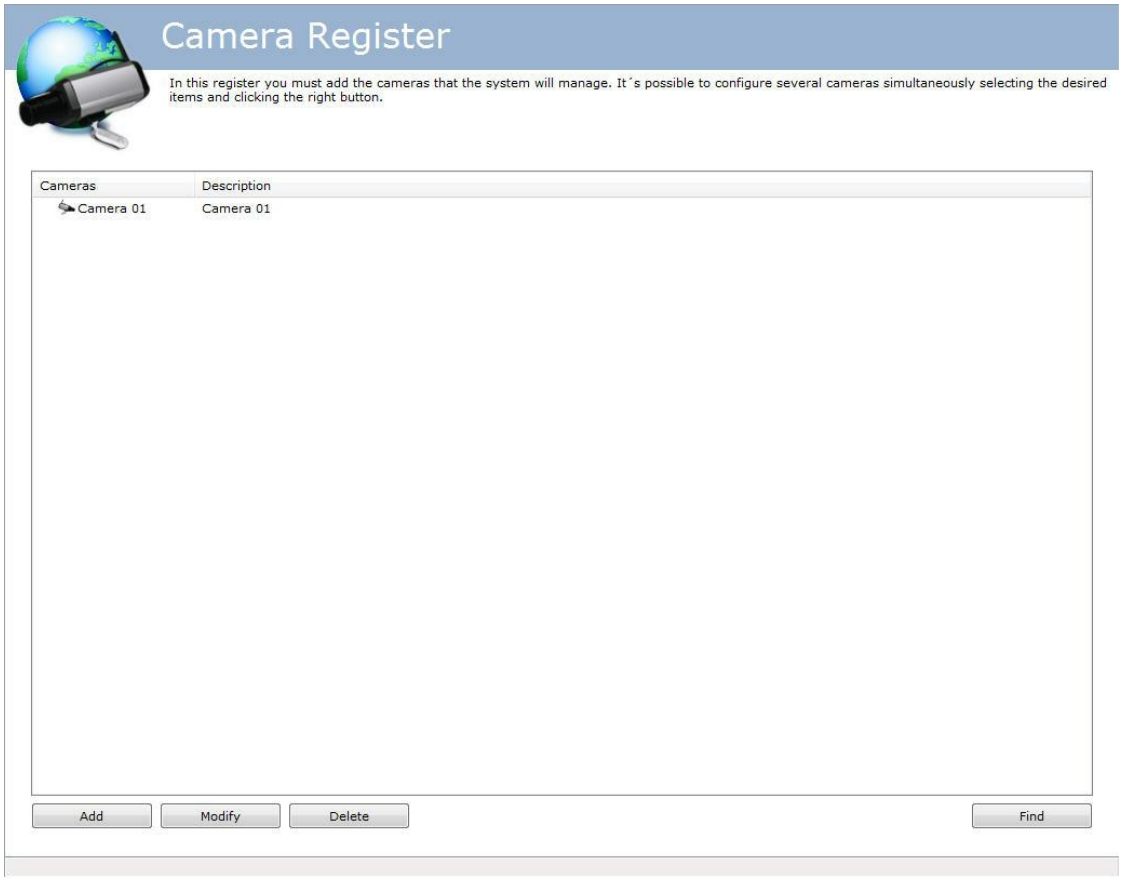
Denies live surveillance rights for the selected cameras. In the option users or groups, a screen will open up with a list of all users or groups registered in the system. Select the users/gruops to whom you want to give the right to video playback for these cameras and click on **OK**. To learn about live surveillance rights see Users rights

6.1.17 Finding and registering cameras automatically

Digifort possess the option to have cameras that support the UPnP protocol to be automatically located and registered into the system. We shall see below how this feature works:

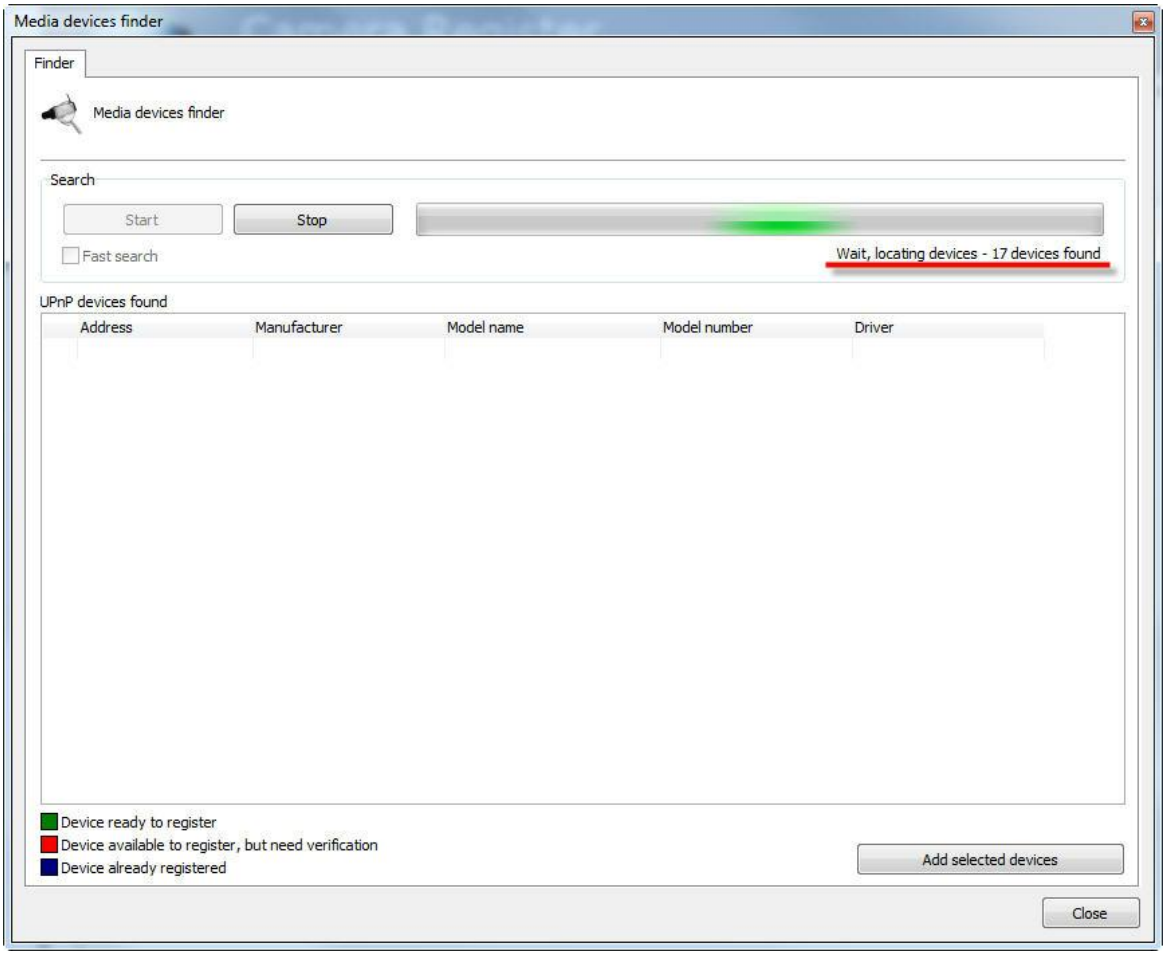
On the screen of camera register click the button (Find) as shown in the image below:

© 2002 - 2011 by Optiview USA all rights


Camera Register
In this register you must add the cameras that the system will manage. It´s possible to configure several cameras simultaneously selecting the desired items and clicking the right button.
Cameras
Description
Camera 01
Camera 01
Add
Modify
Delete
Find

The following screen appears:

© 2002 - 2011 by Optiview USA all rights



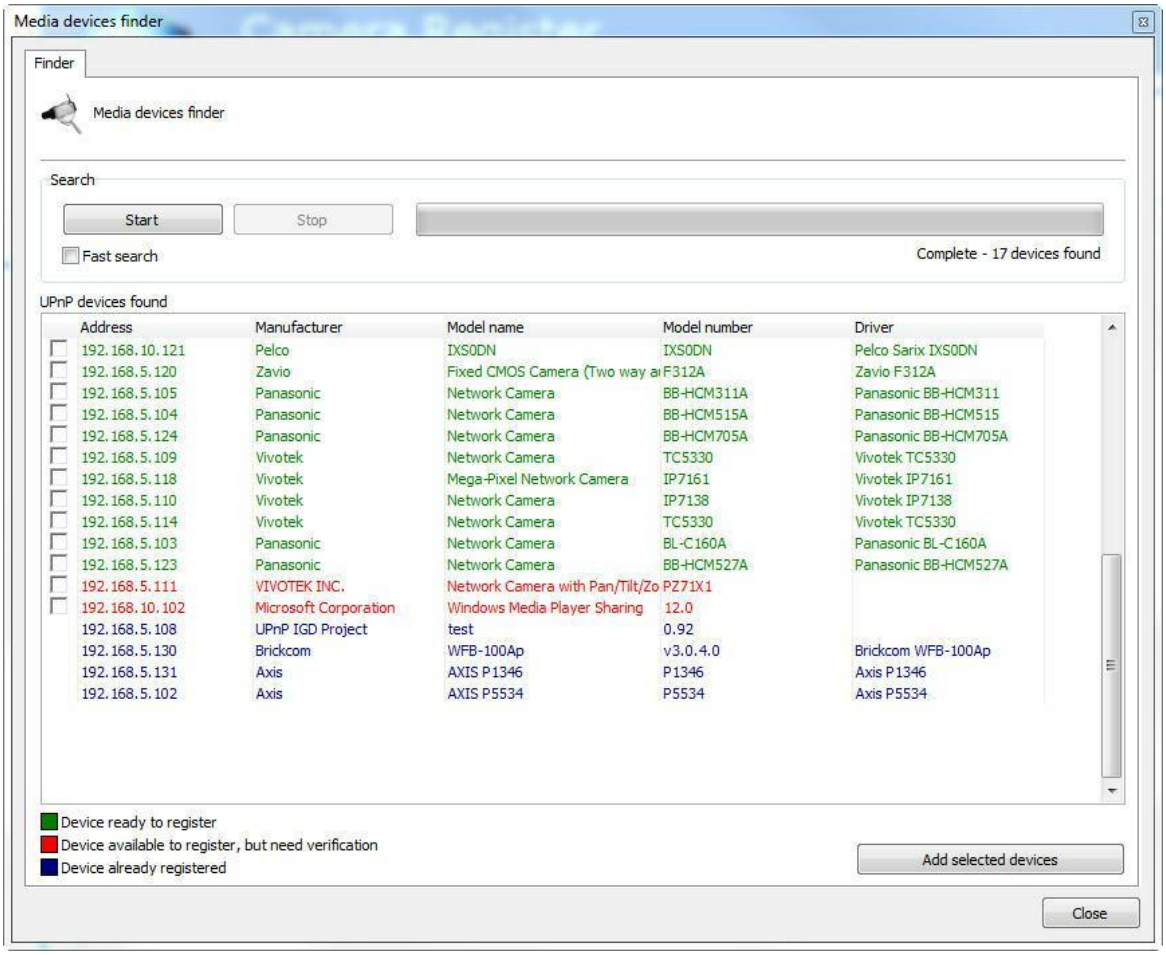
On this screen to search for equipment is made. There are two types of search:

- **Normal** The normal search for UPnP devices takes about 40 seconds to find the equipment. This happens because besides find the equipment that responded to a request, this search looks for UPnP broadcast packets on network to find more devices.
- **Quick Search:** The quick search takes about 15 seconds to finding an equipment. This search only finds devices

who responded to the Digifort UPnP request . To enable quick search simply click on the **Fast Search** box.

To begin your search click on **Start (Start)** button and the message "**wait, location devices** " will appears while the equipment are located. Once found, the equipment will be listed as shown below:

© 2002 - 2011 by Optiview USA all rights

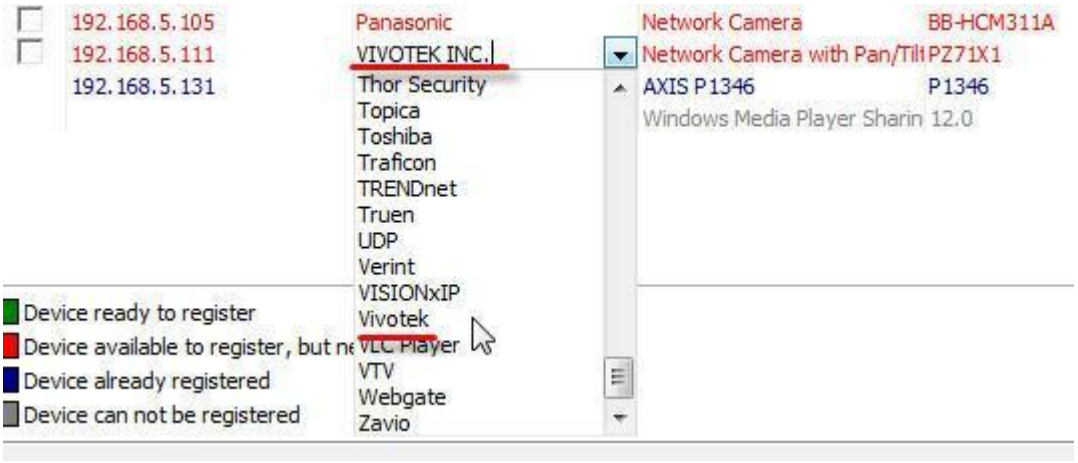

Media devices finder
Finder
Media devices finder
Search
Start
Stop
Fast search
Complete - 17 devices found
UPnP devices found
Address Manufacturer Model name Model number Driver
192.168.10.121 Pelco IXS0DN IXS0DN Pelco Sarix IXS0DN
192.168.5.120 Zavio Fixed CMOS Camera (Two way a F312A Zavio F312A
192.168.5.105 Panasonic Network Camera BB-HCM311A Panasonic BB-HCM311
192.168.5.104 Panasonic Network Camera BB-HCM515A Panasonic BB-HCM515
192.168.5.124 Panasonic Network Camera BB-HCM705A Panasonic BB-HCM705A
192.168.5.109 Vivotek Network Camera TC5330 Vivotek TC5330
192.168.5.118 Vivotek Mega-Pixel Network Camera IP7161 Vivotek IP7161
192.168.5.110 Vivotek Network Camera IP7138 Vivotek IP7138
192.168.5.114 Vivotek Network Camera TC5330 Vivotek TC5330
192.168.5.103 Panasonic Network Camera BL-C160A Panasonic BL-C160A
192.168.5.123 Panasonic Network Camera BB-HCM527A Panasonic BB-HCM527A
192.168.5.111 VIVOTEK INC. Network Camera with Pan/Tilt/Zo PZ71X1
192.168.10.102 Microsoft Corporation Windows Media Player Sharing 12.0
192.168.5.108 UPnP IGD Project test 0.92
192.168.5.130 Brickcom WFB-100Ap v3.0.4.0 Brickcom WFB-100Ap
192.168.5.131 Axis AXIS P1346 P1346 Axis P1346
192.168.5.102 Axis AXIS P5534 P5534 Axis P5534
Device ready to register
Device available to register, but need verification
Device already registered
Add selected devices
Close

It can be found three types of devices according to the subtitles at the bottom left of the screen:

- **Green - (Device ready to register):** These are the cameras that have found their manufacturers and models already approved in Digifort. These cameras devices are ready to be added to Digifort.

- **Red - (Device available to register):** These are the devices that were not found in the data base of approved devices in Digifort. This can occur if the unit is not actually approved or the name of the manufacturer / driver is written differently than is registered in Digifort. In case the name is incorrect, it can be corrected on the screen itself through a selection box as shown below:

© 2002 - 2011 by Optiview USA all rights



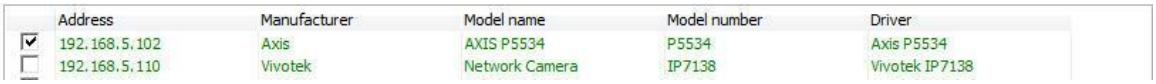
- **Blue - (Device already registered)**: These are devices that are already registered in Digifort.

- **Grey - (Device cannot be registered):** In this case the device or software located did not return any IP address and the device cannot be added automatically.

There are two ways to **register** the devices found.

6.1.17.1 Registration of one device only

- **Registration of one device only:** Select a product over the box as shown below:



	Address	Manufacturer	Model name	Model number	Driver
☑	192.168.5.102	Axis	AXIS P5534	P5534	Axis P5534
☐	192.168.5.110	Vivotek	Network Camera	IP7138	Vivotek IP7138

After selecting the device, click the **Add selected devices** and the camera registration screen is displayed with **Manufacturer**, **Camera model, IP** and **Port** fields already filled. Thus we will only have to fill out name, description, recording directory, and password of the camera.

6.1.17.2 Registration of various devices

This feature can register multiple cameras simultaneously with sequential numbers. To begin, select several devices from the selection box as shown below:



	Address	Manufacturer	Model name	Model number	Driver
☑	192.168.5.102	Axis	AXIS P5534	P5534	Axis P5534
☑	192.168.5.131	Axis	AXIS P1346	P1346	Axis P1346
☑	192.168.5.120	Zavio	Fixed CMOS Camera (Two wa	F312A	Zavio F312A
☑	192.168.5.110	Vivotek	Network Camera	IP7138	Vivotek IP7138
☐	192.168.5.115	3S Vision	Internet Camera		3S Vision N1071

After selecting the device, click the Add selected devices and the following screen appears:

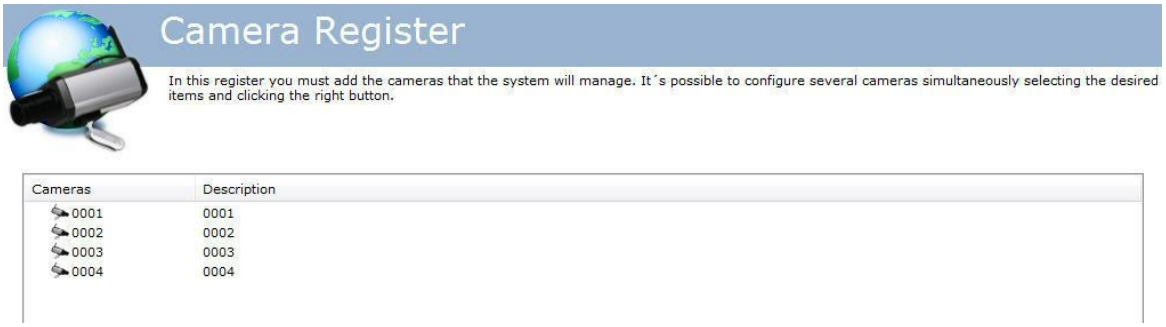
© 2002 - 2011 by Optiview USA all rights



The information provided on this screen will apply for all cameras to be registered:

- **Device initial number:** The name of the cameras will be recorded in the form of a sequence of numbers. This field will set the starting number from which to begin counting.
- **Digit count**: number of spaces you want. E.g.: If the counting starts with number 1 and number of decimal places is 4 then the name of the first camera registered will be 0001.
- **Device username**: User name used for Digifort to authenticate the devices.
- **Device password**: Password used for Digifort to authenticate the devices.
- **Root path for recording:** Enter a directory where Digifort will create a folder for each camera to store your recordings. This folder will have the same camera name (E.g.: 0001, 0002, etc.).

Após cadastrar as diversas câmeras, seus respectivos status automaticamente mudarão para **AZUL (Câmera já cadastrada).** Dessa maneira as câmeras foram cadastradas com sucesso como mostra a imagem abaixo:



© 2002 - 2011 by Optiview USA all rights

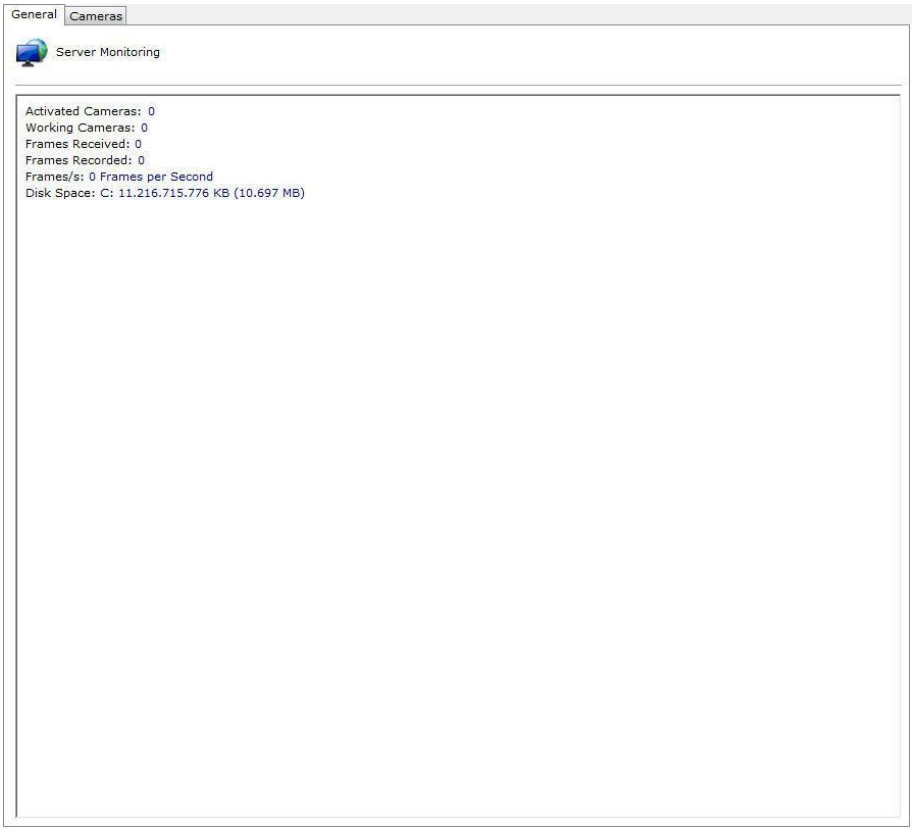
6.2 Monitoring the status of the recording server

In this area of the system you will be able to check up on the general status of all cameras registered in the system

To access this function, select the item Status in Recording Server in the Configurations Menu, as shown in the picture below:



Once this is done, a screen will be opened on the right side with general information about the cameras, as shown in the picture below:

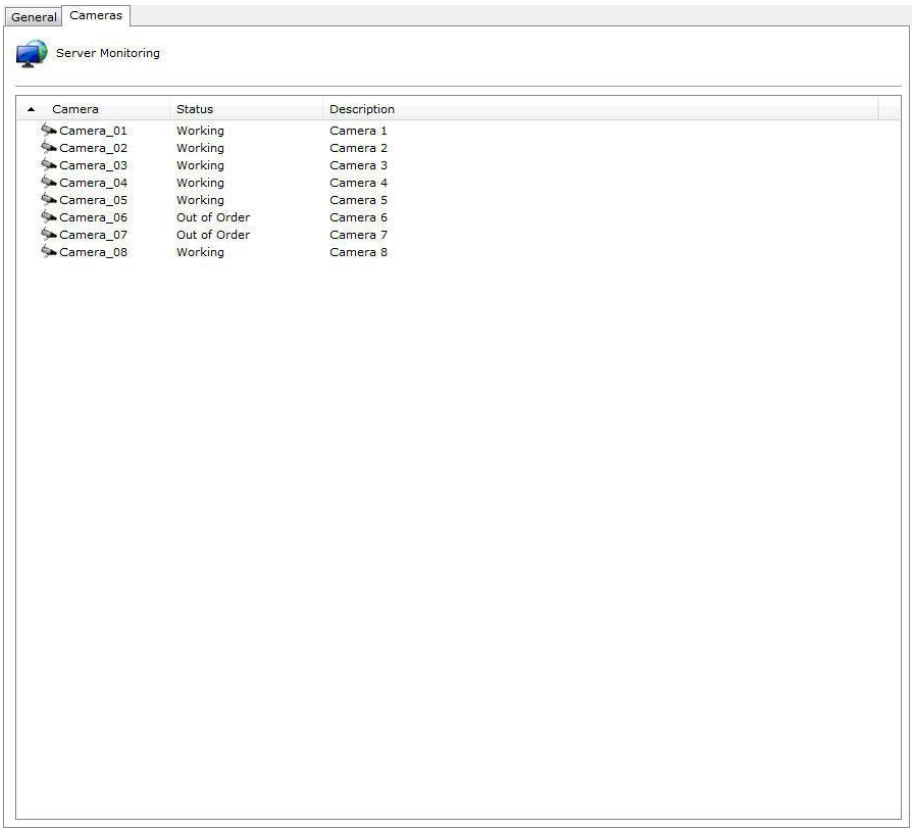


6.2.1 Monitoring the status of cameras individually

In this area of the system you will be able to check up on the individual status of each camera, getting information such as working status, IP address, activity time, disk space used, etc.

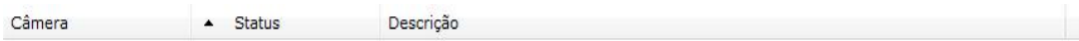
© 2002 - 2011 by Optiview USA all rights

To access this feature, click on the Cameras tab in the Status item of the Recording Server, as shown in the picture below:



This screen will show all of the registered and active cameras in the system and inform us about the working status. If the status is “Working”, the camera is working normally and if the status is “Out of order” some communication problem with the camera is happening, check the electrical and logical net.

The list can be classified by camera names, by their status or by description. To do so, simply click above the desired topic. An arrow will show which topic is being listed and if it’s increasing or decreasing order as shown in the figure.

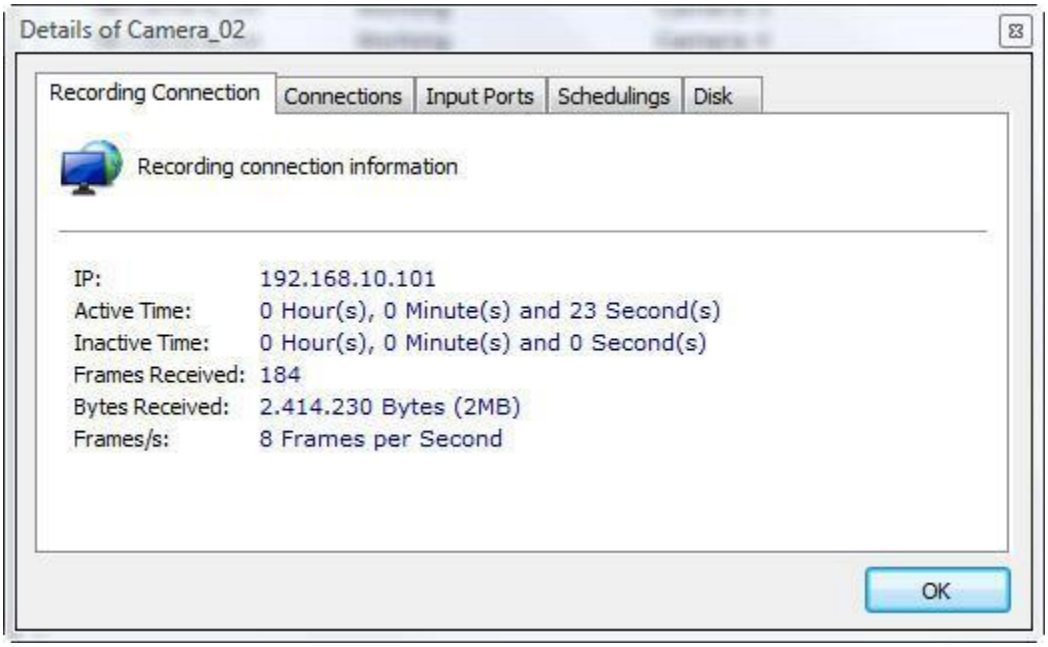


To display details about the functioning of each camera, give a double-click on the desired camera. The details will be described in the next topics.

6.2.1.1 Recording Connection

This screen gives detailed information about the connection used with the camera for image recording, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



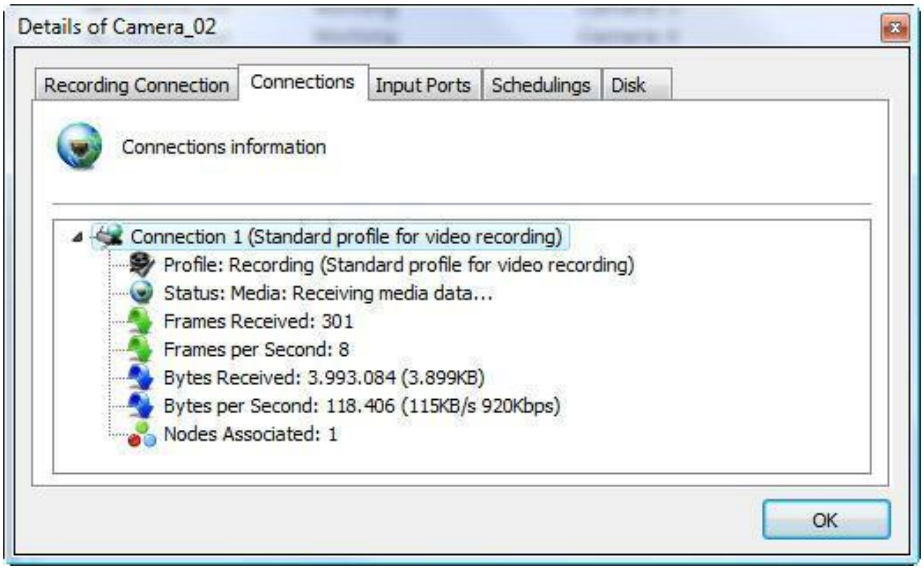
- **IP**: IP address of the camera.
- **Active Time**: Activity time of the camera since its activation or modification of the parameters.
- **Inactive Time**: Inactivity time of the camera.
- **Photos received**: The number of photos received from the camera since its activation or modification of the parameters.
- **Bytes received**: The number of bytes received from the camera since its activation or modification of the parameters.
- **Frames/s:** Frames per second being received from the camera.

6.2.1.2 Connections

This screen gives us information about all connections made with the camera for recording and video visualization.

The connections are displayed in tree-format, that is, showing the type of connection, with items, showing the type of connection, and subitems, displaying details of the connection.
To access this feature, click on the Connections tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights

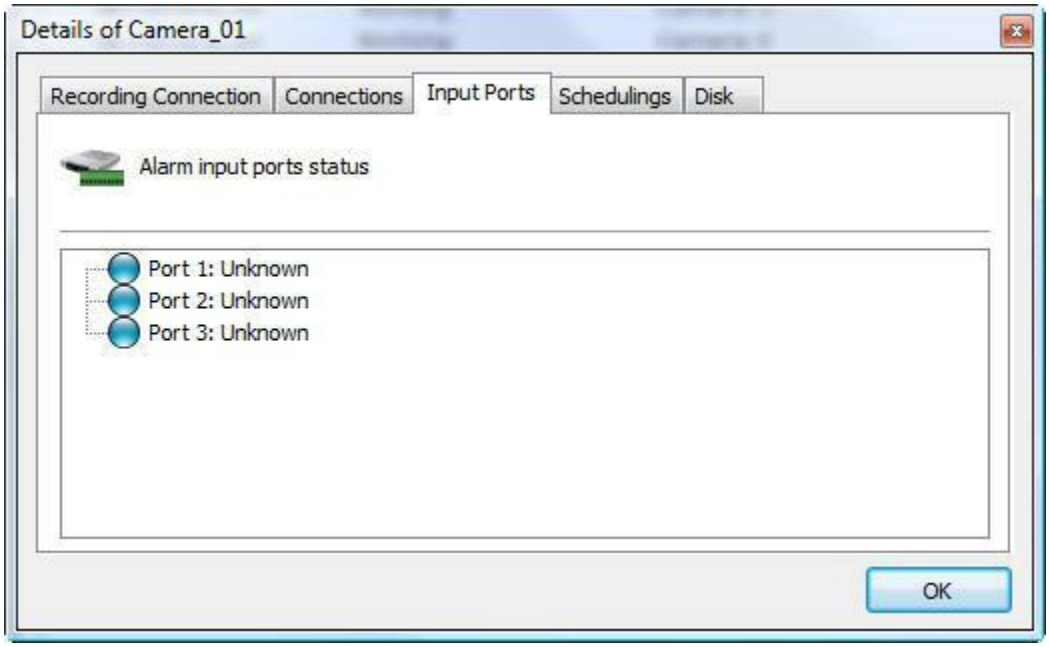


- **Profile**: media profile associated with the connection. To learn what a media profile is, see Media Profiles
- **Frames Received**: Frames received from the camera with this connection since its activation or modification of the parameters.
- **Frames per Second**: Frames per second being received in real time.
- **Bytes Received**: Bytes received from the camera with this connection since its activation or modification of the parameters.
- **Bytes per Second**: Bytes per second being received in real time.
- **Associated Nodes**: The number of features being used in this connection. In this case, the connection is being used only for recording the images, showing the value 1. If the camera were also being monitored via Relay Server by this connection, the value 2 would be displayed.

6.2.1.3 Input Ports

This screen shows the alarm ports of the camera and its Status

© 2002 - 2011 by Optiview USA all rights

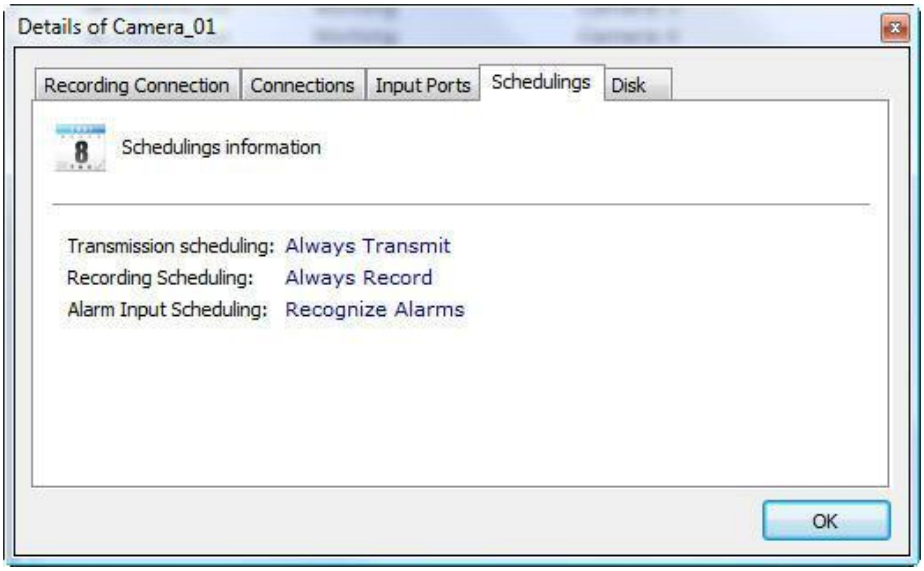


To learn how to configure the alarms see How to configure the alarm actions

6.2.1.4 Schedulings

This screen offers information about the current type of recording, these being: continuous recording, recording by motion, or no recording.

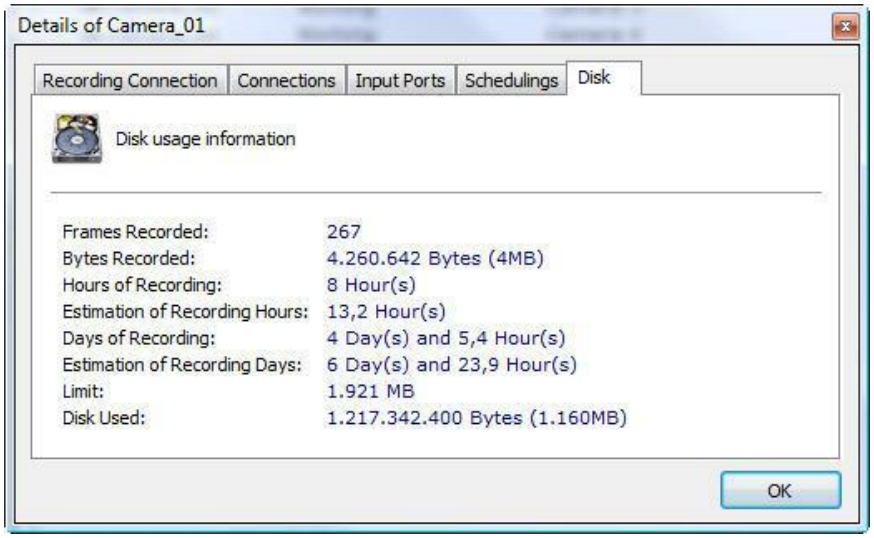
The type of recording is defined in the registration of cameras. To learn how to define the type of recording, see How to configure the recording of the camera. To access this feature, click on the Scheduling's tab, as shown in the picture below:



© 2002 - 2011 by Optiview USA all rights

6.2.1.5 Disk

This screen supplies us with information about disk space usage by this camera.
To access this feature, click on the Disk tab, as shown in the picture below:



For a better understanding of all of these items, read the topic about Disk Management on page How to configure the Disk Management

- **Photos recorded**: The number of photos recorded by the camera since its activation or modification of the parameters.
- **Bytes recorded**: The number of bytes recorded by the camera since its activation or modification of the parameters.
- **Hours of recording**: Hours of recording stored in disk.
- **Estimated hours of recording**: Estimation of the number of hours of recording.
- **Days of recording**: Days of recording stored in disk.
- **Estimated days of recording**: Estimation of the number of days of recording.
- **Limit**: Limit allocated for recording of images of the camera.
- **Disk used**: Disk space used by the images of the camera.

© 2002 - 2011 by Optiview USA all rights

Chapter VII

7 Alarm Devices

The Digifort System allows the management of external alarm devices. Normally, these devices are alarm boards controlled by the network, as are some cameras, and have alarm inputs and outputs that can be monitored by Digifort.

Normally, the alarm devices are installed in places that don't have alarms or the cameras that are installed don't have ports for alarm input and output.

They can be used in automation of an area. Sensors and panic buttons, among other things, can be attached to their input ports. Sirens, electrical locks and lights, among other things, can be attached to their output ports.

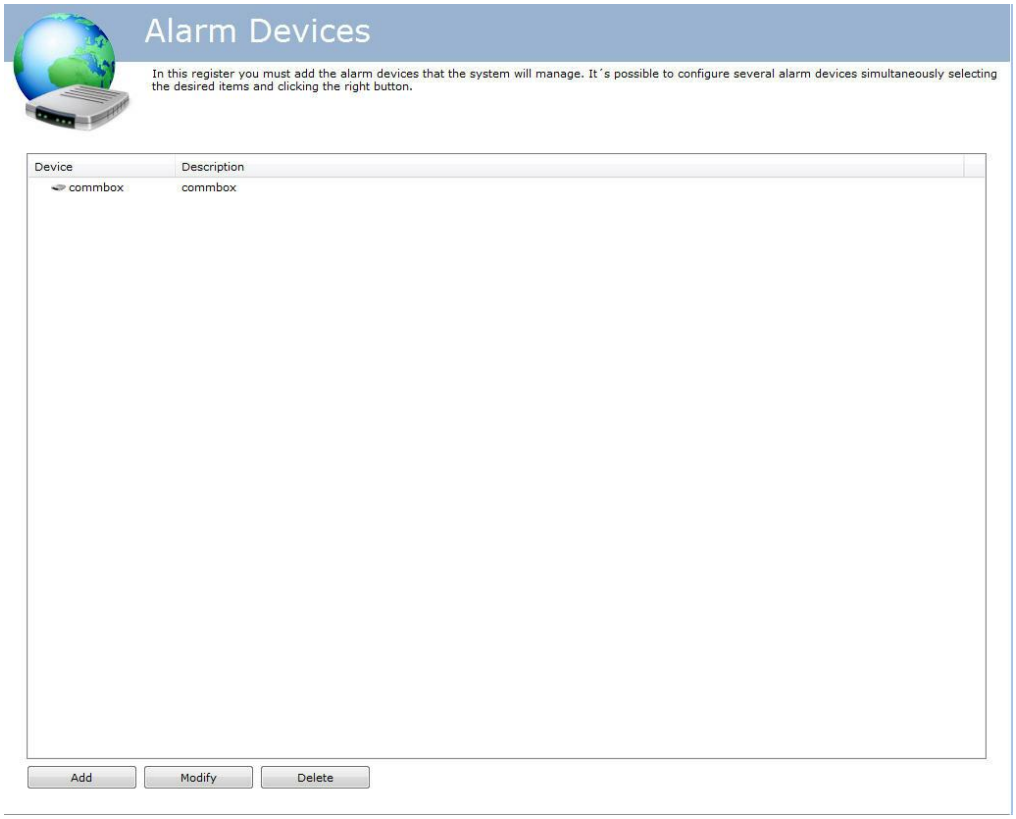
7.1 How to access the alarm devices register

To access the alarm devices register, click on the Devices item in Alarm Devices, as shown in the picture below:



Once this is done, the alarm devices register will be shown on the right, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights


Alarm Devices
In this register you must add the alarm devices that the system will manage. It´s possible to configure several alarm devices simultaneously selecting the desired items and clicking the right button.
Device
Description
commbox
commbox
Add
Modify
Delete

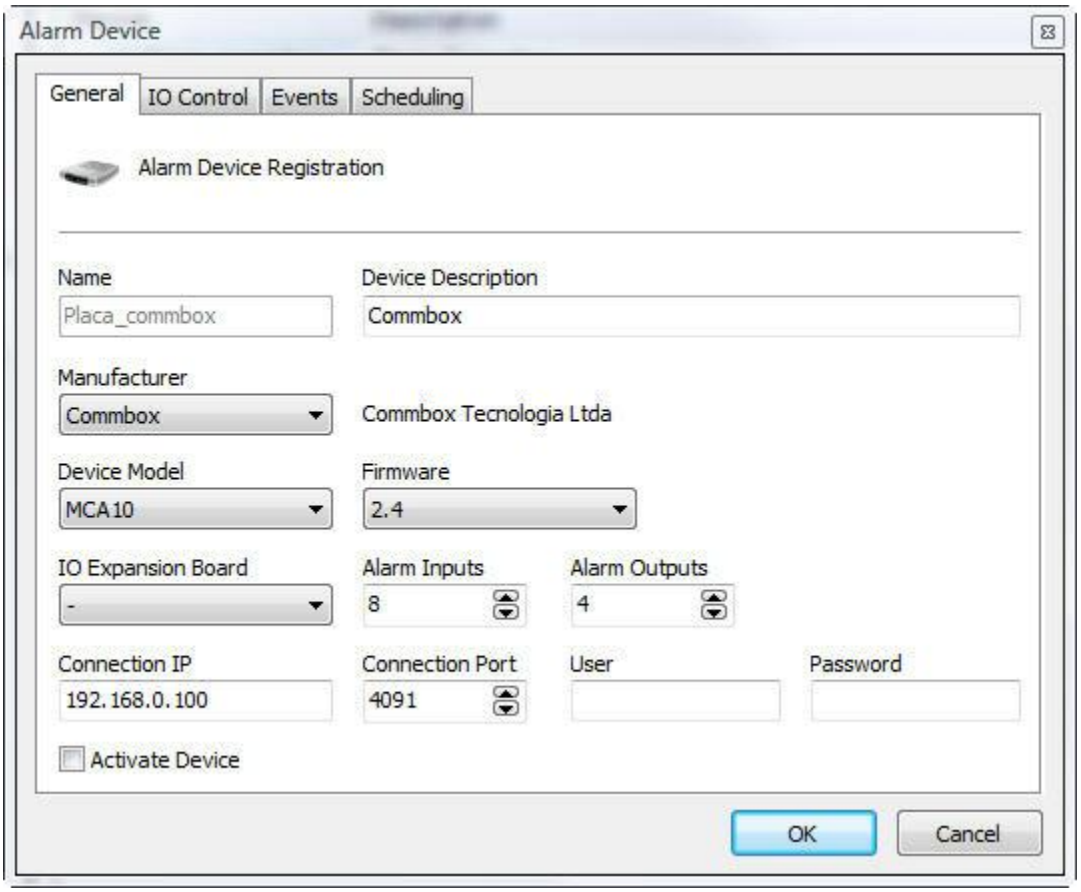
To add an alarm device, click on **Add**. To modify or exclude select the desired alarm device and click on the corresponding button.

7.1.1 How to add an alarm device

After clicking on the **Add** button, as explained in the previous topic, the screen for adding alarm devices will be shown, as shown in the picture below

© 2002 - 2011 by Optiview USA all rights

7.1.1.1 Main data



- **Name**: Identification name of the alarm device. After inclusion of the device in the system, the name cannot be modified, as it will be used internally by the system.
- **Description of the device**: Brief description of the alarm device.
- **Manufacturer**: Select the manufacturer of the alarm device.
- **Model of the device**: Select the model of the alarm device.
- **I/O expansion board**: If your device has a port expansion board, select it from this list.
- **Alarm inputs**: Select the number of alarm input ports the device has.
- **Alarm outputs**: Select the number of alarm output ports the device has.
- **Connection IP**: Enter the IP of the connection with the alarm device.
- **Connection port**: Enter the port of the connection with the alarm device.
- **User**: Enter the user of the access to the alarm device.
- **Password**: Enter the password of the access to the alarm device.

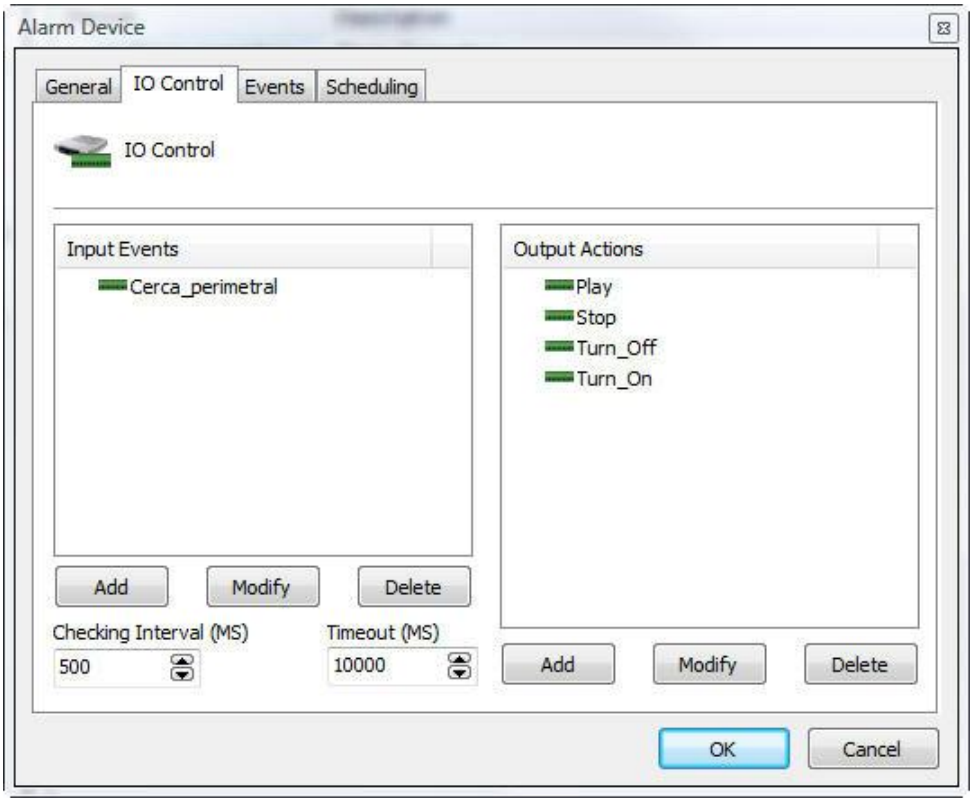
Important

To find out the IP and port of the connection, and the user and password of access, consult the alarm device's instructions manual.

© 2002 - 2011 by Optiview USA all rights

7.1.1.2 I/O Control

In this area the alarm device will be configured. To access these configurations, click on the I/O Control tab, as shown in the picture below:



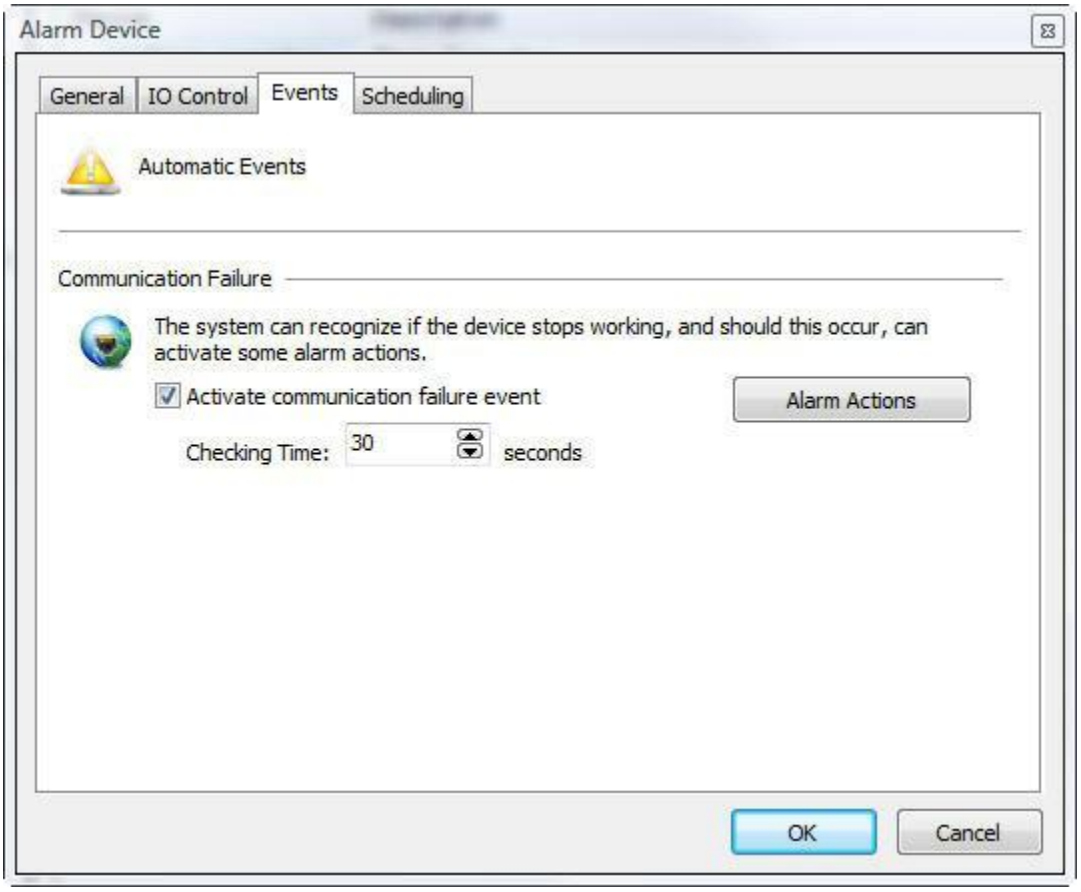
To learn how to use this screen, see **How to configure the I/O**

7.1.1.3 Events

As in the case of cameras, Digifort can also monitor the working state of the alarm devices, offering notification functions, in case the equipment stops functioning for any reason.

Digifort can inform the administrator of failures in communication with the alarm device that can be caused by lack of power at the site, or signs of vandalism, for example. To access this feature, click on the **Events** tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



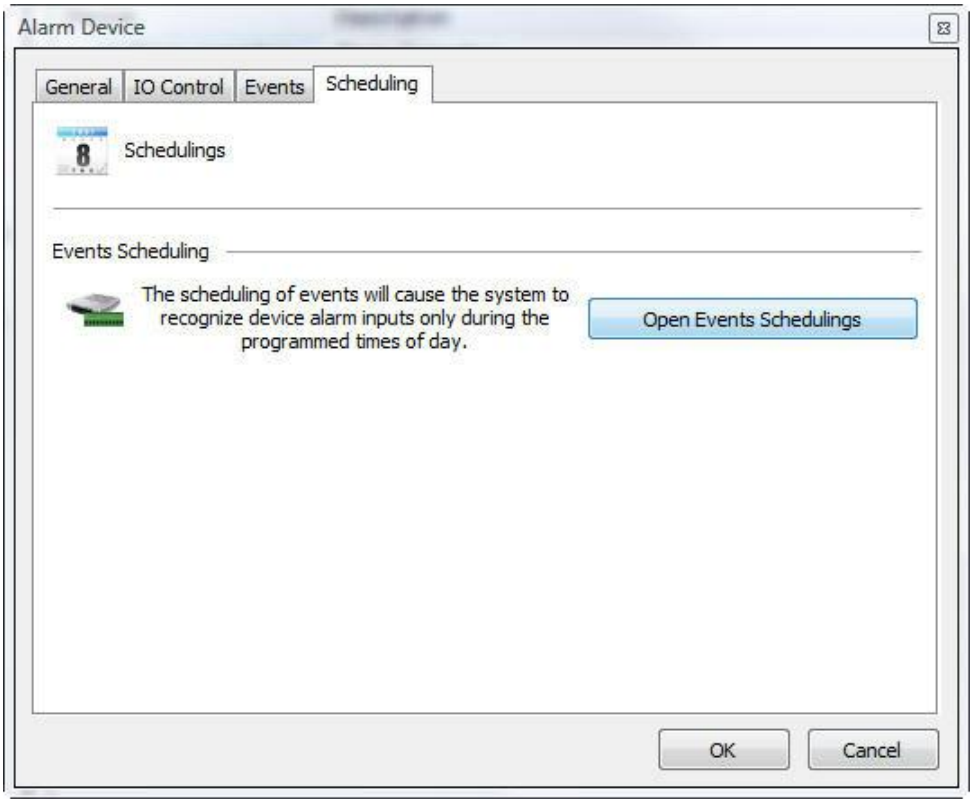
If you wish to activate this notification, mark the option Activate communications failure event and define the time for checking. This time defines the interval after which Digifort verifies if there is connection with the device. For this, click on Alarm Actions to define the set of actions that Digifort will carry out when this event occurs. To learn how to configure the alarm action, see How to configure the alarm actions

7.1.1.4 Scheduling

Scheduling makes it possible for the administrator to configure the times of day and days of the week in which the events received by the alarm devices are to be processed. For example, a rule can be defined that the events will only be processed at night.

To access this feature, click on the Scheduling tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights

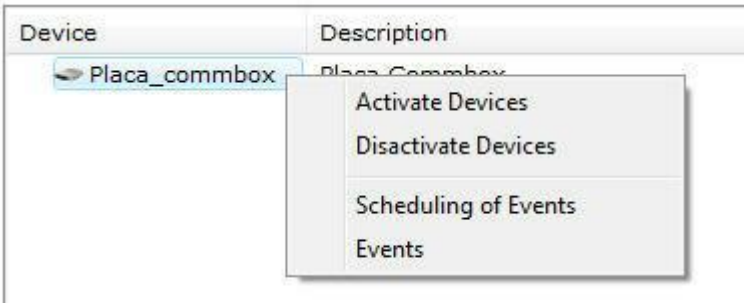


To configure the scheduling, click on Open Scheduling of Events and follow the instruction on page How to configure the scheduling of recording

7.1.2 Management functions of the Alarm Devices

Digifort offers the principal configurations of alarm devices that can be accessed based on its register, thus making it possible to configure several devices simultaneously.

To use this feature, select the desired devices and click on the right button of the mouse, as shown in the picture below:



- **Activate devices**: Activates the selected devices, causing the alarms to be administrated.
- **Disactivate devices**: Disactivates the selected devices.
- **Scheduling of events**: Configures the scheduling of events of the selected device. To learn how to use this feature, see Events.

© 2002 - 2011 by Optiview USA all rights

- **Events**: Configures the events of the selected devices. To learn how to use this feature, see I/O Control

© 2002 - 2011 by Optiview USA all rights

Chapter VIII

8 Alerts and Events

The Digifort System offers a series of alerts and alarms that can help to monitor the normal operation of a set of cameras and the server itself. These alerts are configured by the system's administrator, according to the individual needs of each solution, and can be modified at any moment whenever a new need appears.

The functions of alerts and events allows Digifort to send e-mail or SMS messages to a list of users that was previously registered in the system each time some event Programmed by the administrator occurs. An event can be, among others, a failure in the communication of the camera with the server, a failure in the recording of data, a motion alert or an alert associated with an external electrical device. All of the alerts are also registered in a log file for later consultation and analysis.

The alerts and alarms are activated immediately following their configuration, making it unnecessary to paralyze the system to accomplish a configuration. An alert can be made for the entire system or for a specific camera.
The monitoring of these alerts is the responsibility of the person to whom the administrator delegated the control.

The lack of interest in checking up on abnormalities detected and informed by the system is considered a serious failure, putting security as a whole at risk.

8.1 How to access the Alerts and Events

To access the alerts and events, click on the item Alerts and Events in the Configurations Menu, as shown in the picture below:



This area of the system is divided into three parts, the contacts register, the contact groups register and the log configuration.

© 2002 - 2011 by Optiview USA all rights

8.1.1 How to configure the contacts

Contacts are system units that are responsible for alert e-mail messages from the system. In other words, contacts are people who are registered in the system with information such as name, telephone and e-mail address. By way of this information, Digifort is able to contact them.

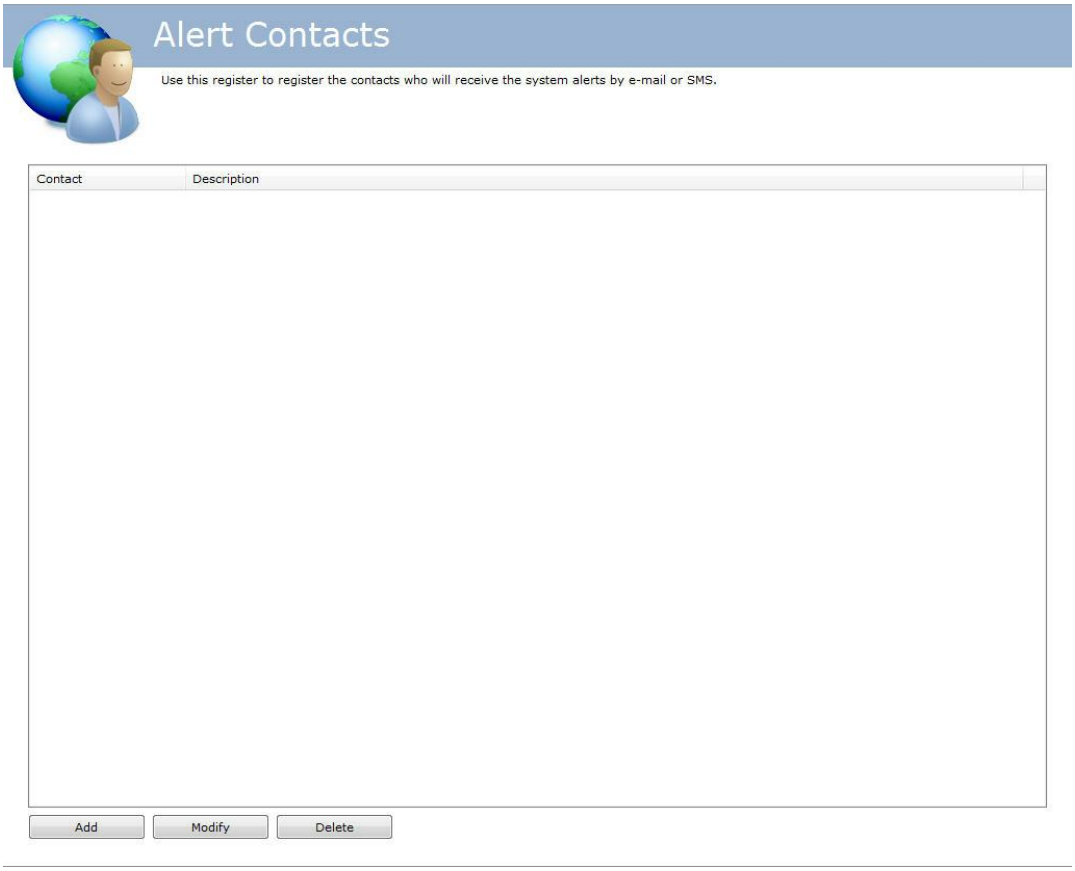
Digifort sends e-mail messages not only to a contact, but also to groups of contacts.

To access the contacts register, click on the item Contacts, as shown in the picture below:



Once this is done, the contacts register will be displayed on the right, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights

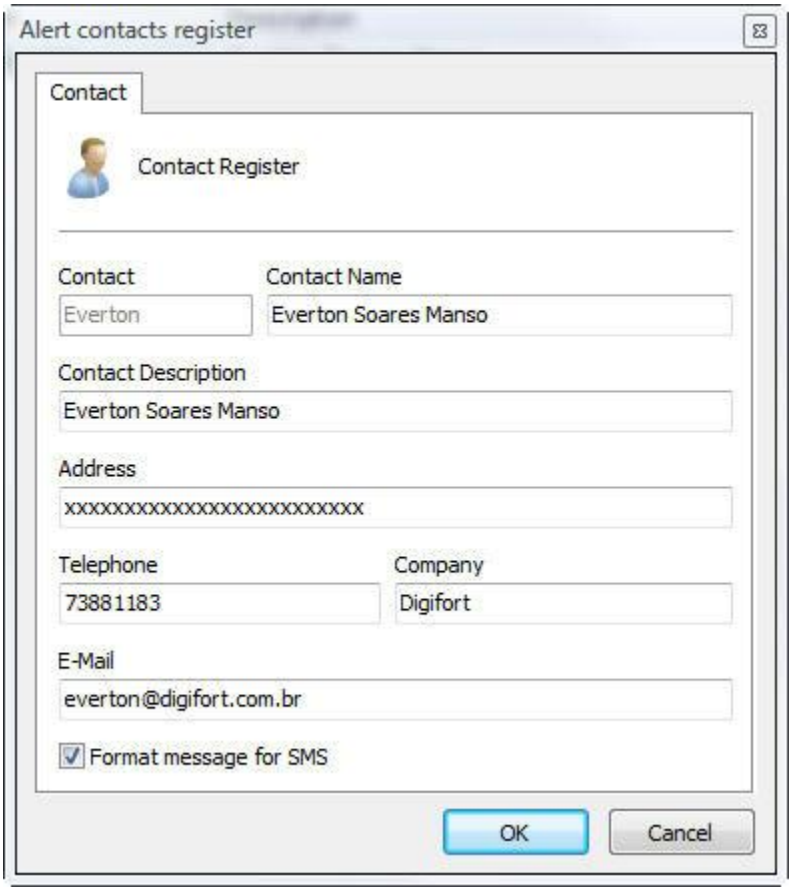


To add a contact, click on the **Add** button. To modify a contact, select it and click on the **Modify** button. To exclude a contact, select it and click on the **Exclude** button.

8.1.1.1 How to add a contact

After clicking on the Add button, as explained in the previous topic, the screen for adding contacts will be displayed, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



- **Contact**: Internal name of the contact. This name must be unique and cannot be modified once saved, as this information in used internally by the system.
- **Name of the contact**: Complete name of the contact.
- **Description of the contact**: A brief description of the contact for the purpose of its easy identification. This field may contain, for example, the function of the person in the company.
- **Address**: Address of the contact.
- **Telephone**: Telephone of the contact.
- **Company**: Company of the contact.
- **E-mail**: E-mail address of the contact. It is to this address that Digifort will send the notifications configured by the administrator.
- · **Format message for SMS**: Sends the notification to cell phone in SMS format instead of by e-mail. In this case the e-mail address of the cell phone must be specified in the field “E-mail”.

Important

The sending of SMS messages is a service out of the realm of Digifort and is therefore the responsibility of the operator of the cell phone who will receive the message. Verify the availability of this service with your operator.

© 2002 - 2011 by Optiview USA all rights

8.1.1.2 How to configure the event logs

The event logs register the events of failure of communication with the cameras and failures in the recording in disk of images coming from the cameras for later visualization and analysis by the system administrator.

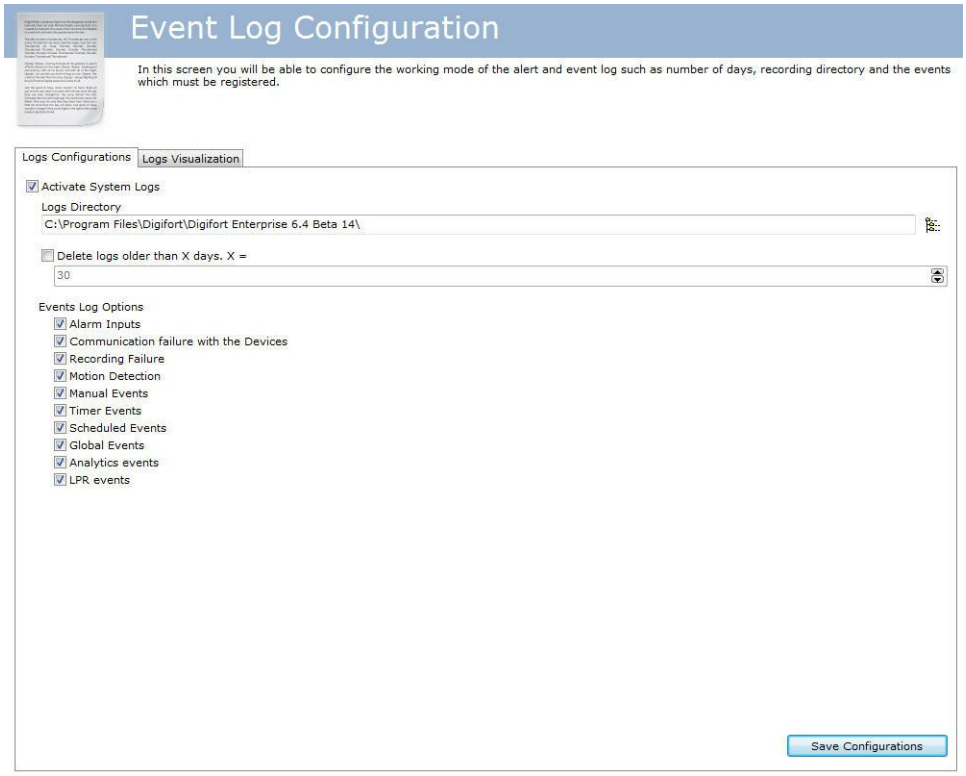
In addition to registering occurrences in the log, it's also possible to execute some actions defined by the administrator, such as the sending of notification e-mail or execution of alarm sounds for the operator, for example. To learn how to do this configurations see How to configure the contact groups

To access this feature, click on the item Logs, as shown in the picture below:



Once this is done, the screen for configuration of alert and event logs will be displayed at the right, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights


Event Log Configuration
In this screen you will be able to configure the working mode of the alert and event log such as number of days, recording directory and the events which must be registered.
Logs Configurations
Logs Visualization
Activate System Logs
Logs Directory
C:\Program Files\Digifort\Digifort Enterprise 6.4 Beta 14\
Delete logs older than X days. X =
30
Events Log Options
Alarm Inputs
Communication failure with the Devices
Recording Failure
Motion Detection
Manual Events
Timer Events
Scheduled Events
Global Events
Analytics events
LPR events
Save Configurations

- **Activate system logs**: Activates Digifort's alert and event logs.
- **Logs Directory**: Selects the directory in which the alert and event logs will be saved.
- **Eliminate logs older than X days**: Eliminates old logs, specified by the informed number of days.
- **Event log options**:
  - **Alarm inputs**: Logs the occurrences of alarm inputs of some device such as the detection of motion in the presence sensor.
  - **Failure in communication with the devices**: Logs the failures of communication with the cameras.
  - **Failure in recording:** Logs the failures in recording in disk of images coming from the cameras.
  - **Motion detection**: Logs the occurrences of motion detection in some camera.
  - **Manual events:** Logs the occurrences of manual events set off by the operator such as, for example, the opening of an electrical lock.
  - **Timer events**: Logs the occurrences of timer events.
- **Save Configurations button:** Saves the configurations specified here.

8.1.1.2.1 How to visualize the event logs

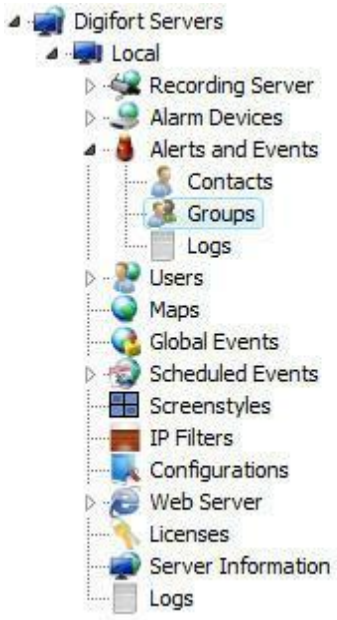
To learn how to visualize the event logs, see How to visualize the event logs

© 2002 - 2011 by Optiview USA all rights

8.1.2 How to configure the contact groups

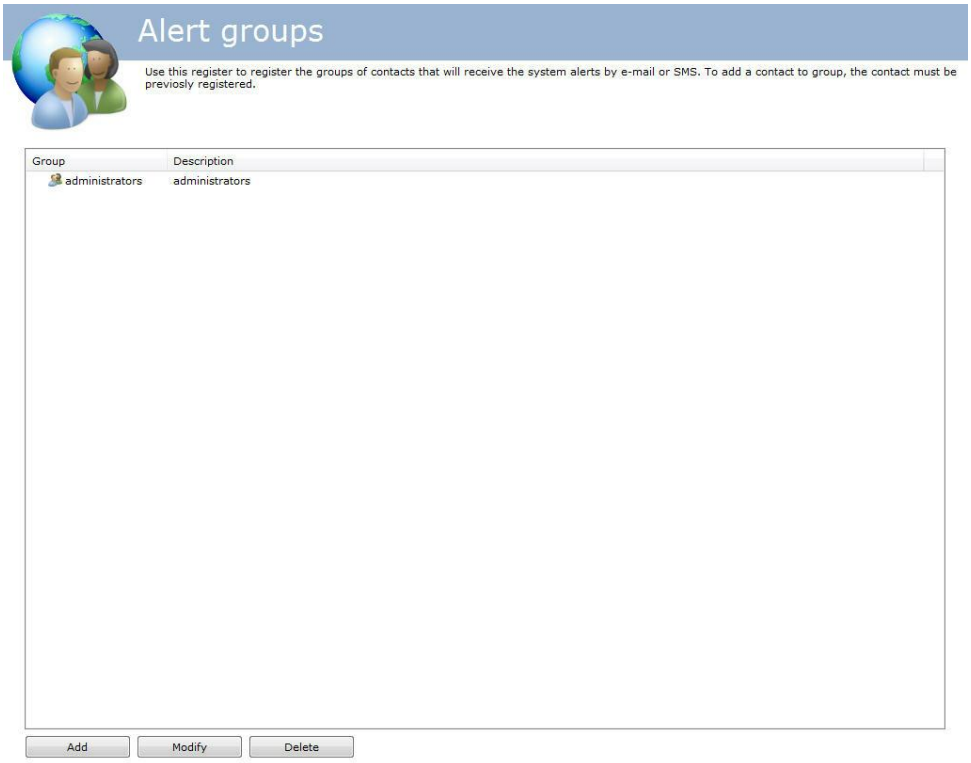
The creation of contact groups is necessary, since Digifort sends e-mail notifications not only to a contact, but also to a group of contacts.

To access the contact groups register, click on the item Groups, as shown in the picture below:



Once this is done, the group register will be displayed at the right, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights

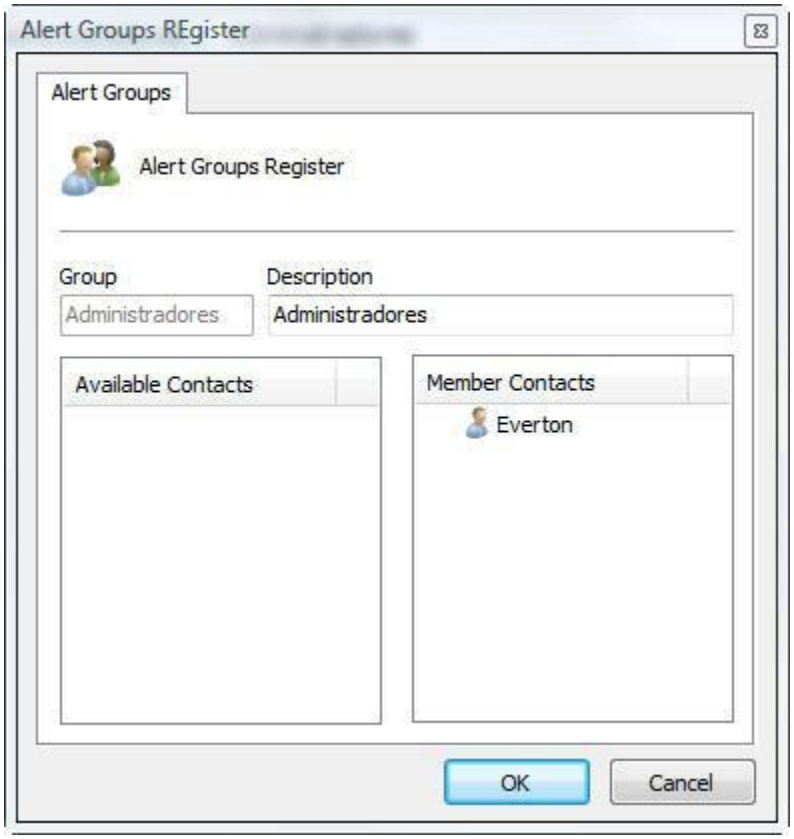

Alert groups
Use this register to register the groups of contacts that will receive the system alerts by e-mail or SMS. To add a contact to group, the contact must be previosly registered.
Group
Description
administrators
administrators
Add
Modify
Delete

To add a contact group, click on the **Add** button. To modify a contact group, select it and click on the **Modify** button. To exclude a contact group, select it and click on **Exclude**.

8.1.2.1 How to add a contact group

After clicking on the **Add** button, as explained in the previous topic, the screen for adding contact groups will be displayed, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



- **Group**: Name of the contact group. Once saved, this name cannot be modified, as it will be used internally by the system.
- **Description**: Description of the contact group.
- **Available contacts**: List of all contacts registered in the system.
- **Member contacts**: List of all contacts who are members of the group.

To add contacts to the group, select the desired contact in the list of available contacts and drag it to the list of member contacts.

To remove a contact from the group, select the desired contact in the list of member contacts and drag it to the list of available contacts.

8.1.3 How to configure the event logs

The event logs register the events of failure of communication with the cameras and failures in the recording in disk of images coming from the cameras for later visualization and analysis by the system administrator.

In addition to registering occurrences in the log, it's also possible to execute some actions defined by the administrator, such as the sending of notification e-mail or execution of alarm sounds for the operator, for example. To learn how to do this confiration see How to configure the contact groups

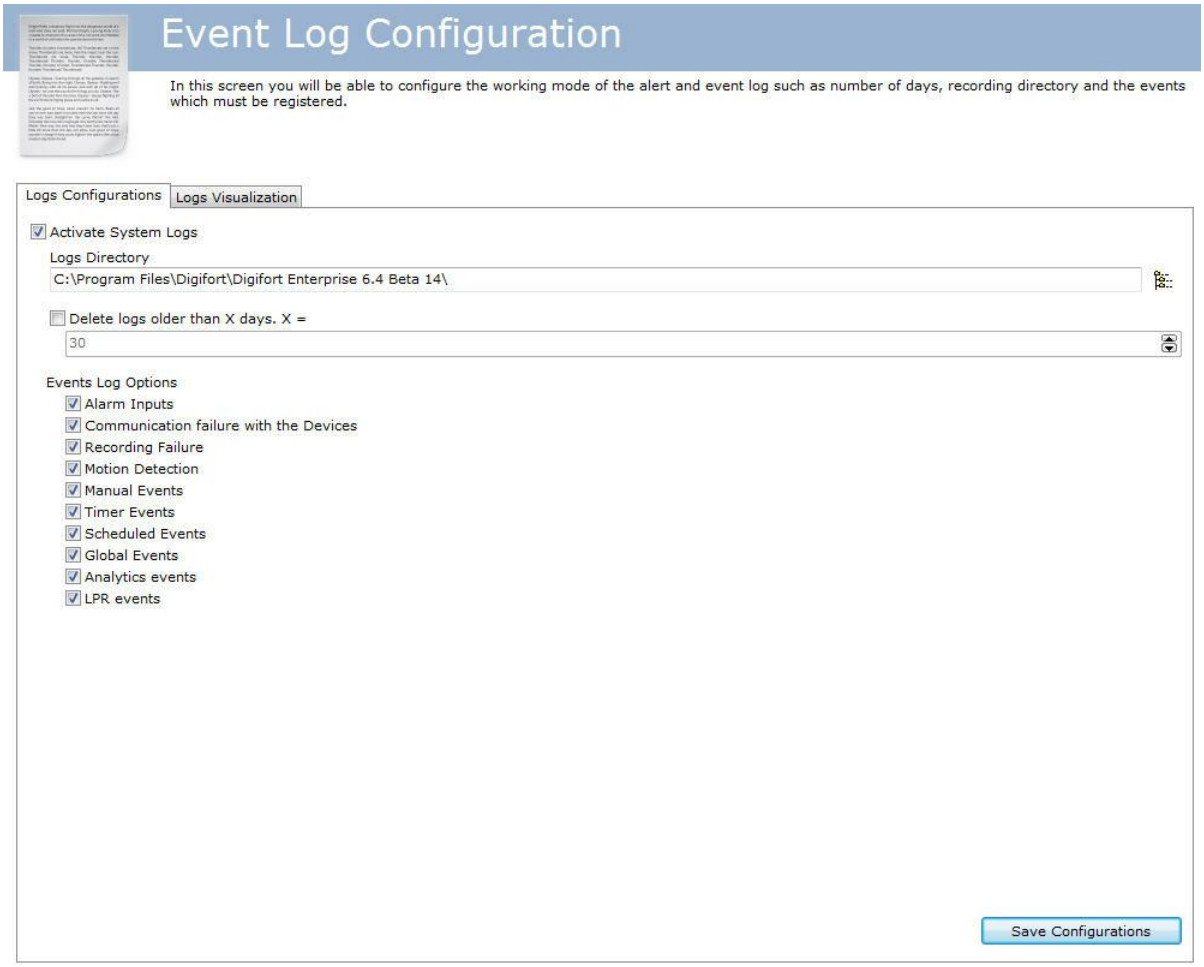
To access this feature, click on the item Logs, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



Once this is done, the screen for configuration of alert and event logs will be displayed at the right, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights


Event Log Configuration
In this screen you will be able to configure the working mode of the alert and event log such as number of days, recording directory and the events which must be registered.
Logs Configurations
Logs Visualization
Activate System Logs
Logs Directory
C:\Program Files\Digifort\Digifort Enterprise 6.4 Beta 14\
Delete logs older than X days. X =
30
Events Log Options
Alarm Inputs
Communication failure with the Devices
Recording Failure
Motion Detection
Manual Events
Timer Events
Scheduled Events
Global Events
Analytics events
LPR events
Save Configurations

8.1.3.1 Activate system logs

Activates Digifort's alert and event logs.

8.1.3.2 Logs Directory

Selects the directory in which the alert and event logs will be saved.

8.1.3.3 Eliminate logs older than X days

Eliminates old logs, specified by the informed number of days.

8.1.3.4 Event log options

8.1.3.4.1 Alarm inputs

Logs the occurrences of alarm inputs of some device such as the detection of motion in the presence sensor.

© 2002 - 2011 by Optiview USA all rights

8.1.3.4.2 Failure in communication with the devices

Logs the failures of communication with the cameras

8.1.3.4.3 Failure in recording

Logs the failures in recording in disk of images coming from the cameras.

8.1.3.4.4 Motion detection

Logs the occurrences of motion detection in some camera.

8.1.3.4.5 Manual events

Logs the occurrences of manual events set off by the operator such as, for example, the opening of an electrical lock

8.1.3.4.6 Timer events

Logs the occurrences of timer events.

8.1.3.4.7 Programmed events

Registers the occurrence of programmed events in the log.

8.1.3.4.8 Global events

Registers the occurrence of global events in the log.

8.1.3.4.9 Eventos de analítico

Registers the occurrence of analytics events in the log.

8.1.3.4.10 LPR events

Registra no log as ocorrências os eventos de LPR

8.1.3.5 Save Configurations button

Saves the configurations specified here.

8.1.4 How to visualize the event logs

To learn how to visualize the event logs, see How to visualize the event logs

© 2002 - 2011 by Optiview USA all rights

Chapter IX

9 User administration

A security system really only works if it has functions and administration capable of making it resistant to vulnerabilities and technical problems during its operation.

The creation of users is very important for the good organization and security of the Digifort Server.

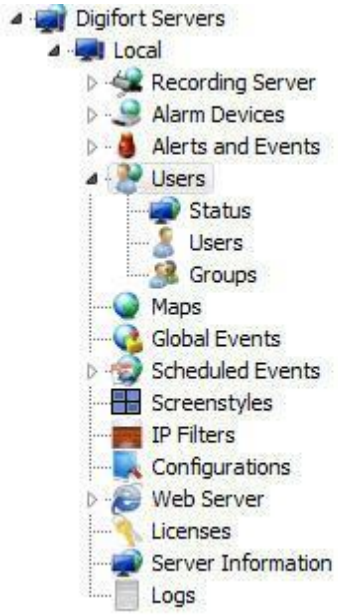
The system's administrator must define a set of users who are responsible for the monitoring and correction of events related to the operation of the Digifort System. With time, these users are automatically notified by the system regarding the conditions and abnormalities that occur and that were defined by the organization as worthy of checking out. An abnormal situation would be a camera that stopped working, or a vault that alerted about someone's undue entry, for example.

These users must be of the utmost trust to the company, as a security solution only works with trustworthy equipment and personnel.

Digifort Enterprise offers the administration of up to eight users, the user admin, which comes previously registered, with all access rights and that cannot be removed, and seven other users to be created.
The user administrator of Digifort is divided into two parts: Status, where the activity of users in the server can be monitored, and Users, where system users can be included, modified and excluded from the system.

9.1 Administrating users

To access the area of user administration, locate the **Users** item in the Configuration Menu of the server to be administrated and give a double-click. The item will be expanded, showing the Status and Users options, as shown in the picture below:

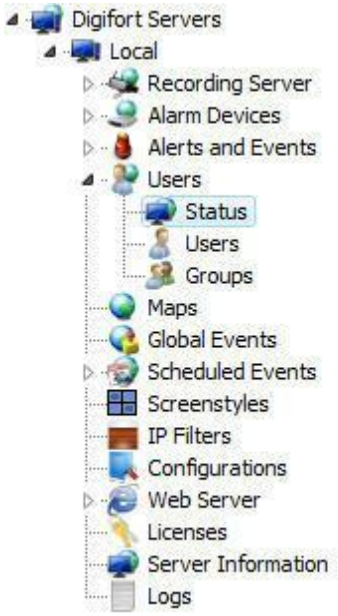


© 2002 - 2011 by Optiview USA all rights

9.1.1 Monitoring user activity

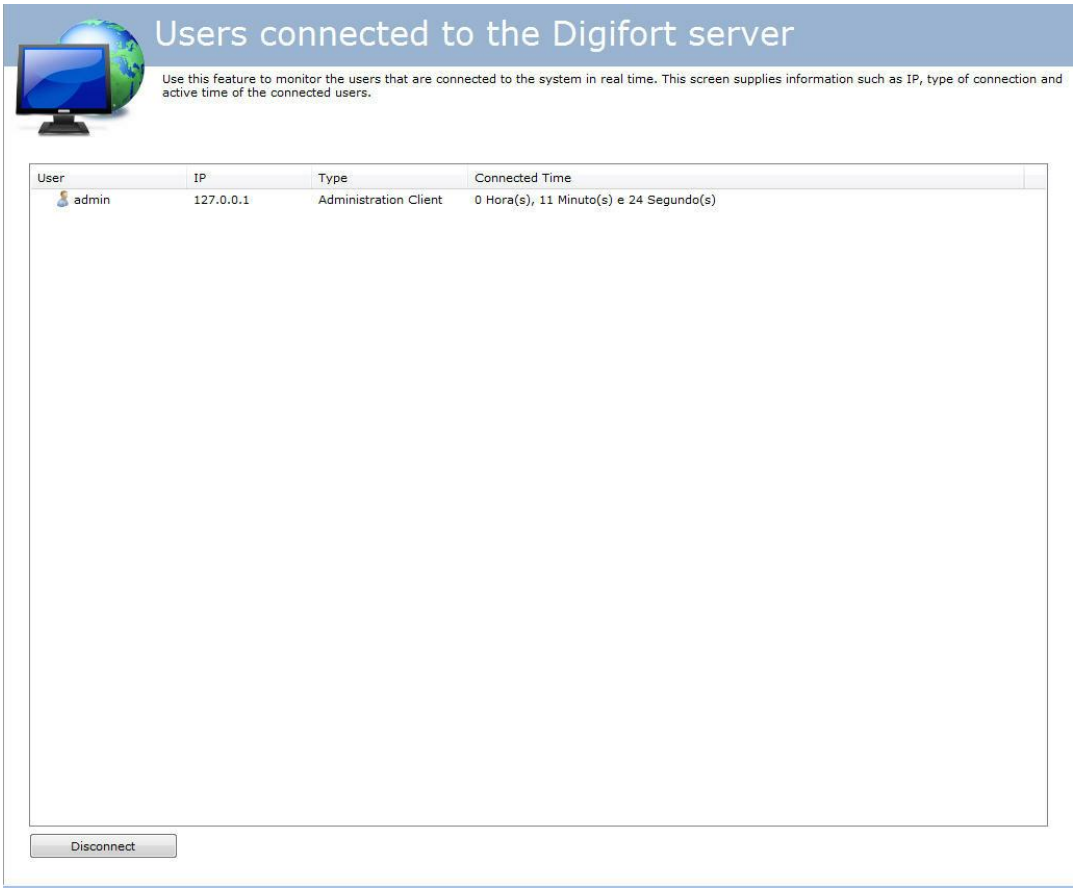
This feature is very important for the security of the server, since logged-in users' activity is monitored here. If the user is taking an undue action, he can be disconnected or blocked.

To access this feature, locate the Status item in the Users item in the Configurations Menu of the server, as shown in the picture below:



Once this is done, the system user activity screen will be opened on the right, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights


Users connected to the Digifort server
Use this feature to monitor the users that are connected to the system in real time. This screen supplies information such as IP, type of connection and active time of the connected users.
User
IP
Type
Connected Time
admin
127.0.0.1
Administration Client
0 Hora(s), 11 Minuto(s) e 24 Segundo(s)
Disconnect

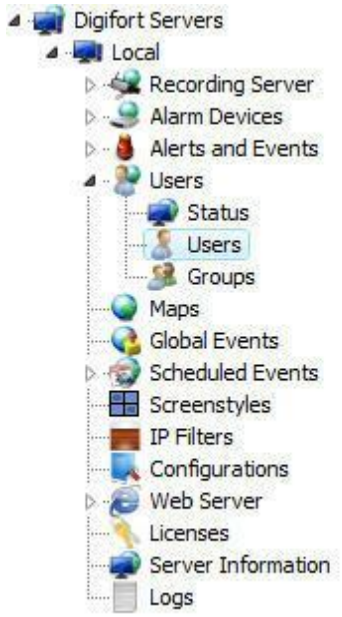
All presently logged-in users of the system are displayed, showing information such as user name, IP address, server access type, and connection time.

To disconnect a user, select the user and click on the **Disconnect** button.

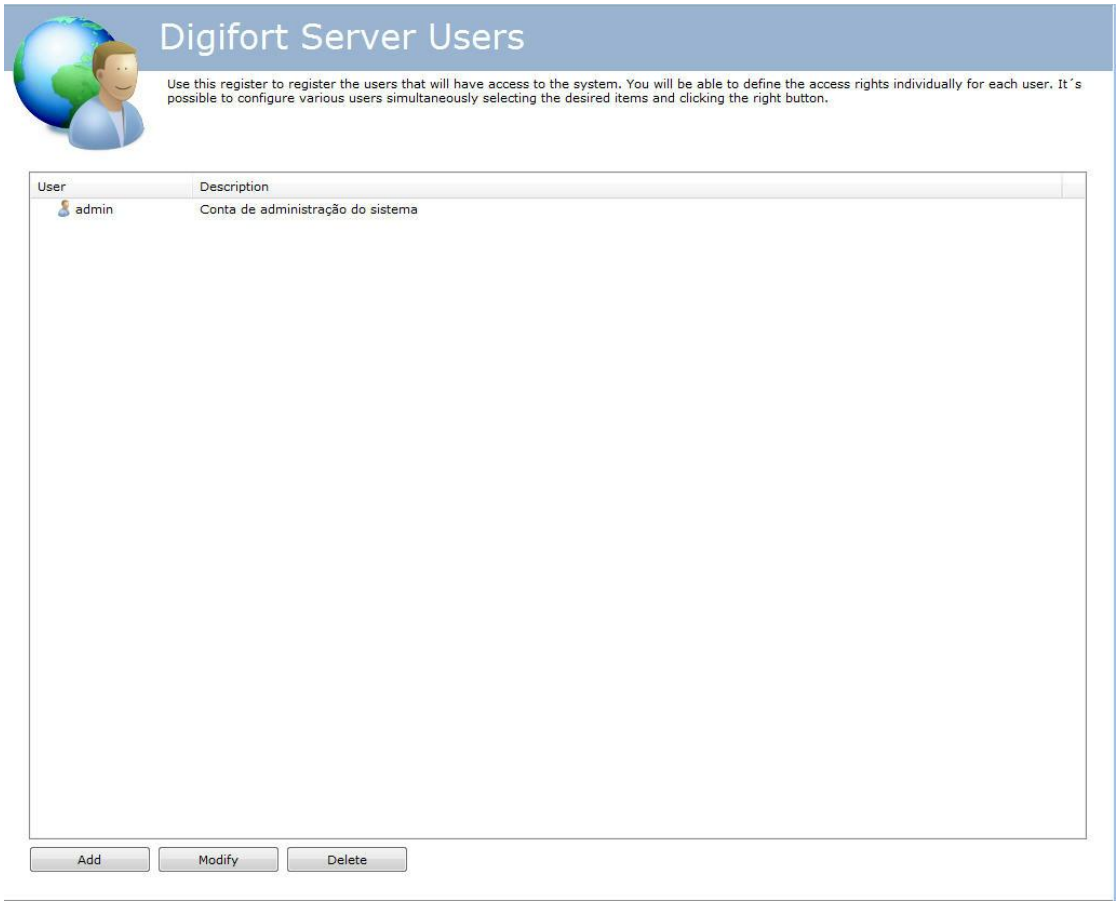
9.2 Adding, modifying and excluding users

To access the user administration, locate the Users item in the Configurations Menu of the server, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



Once this is done, the user administration screen will be opened on the right side, as shown in the picture below:


Digifort Server Users
Use this register to register the users that will have access to the system. You will be able to define the access rights individually for each user. It´s possible to configure various users simultaneously selecting the desired items and clicking the right button.
User
Description
admin
Conta de administração do sistema
Add
Modify
Delete

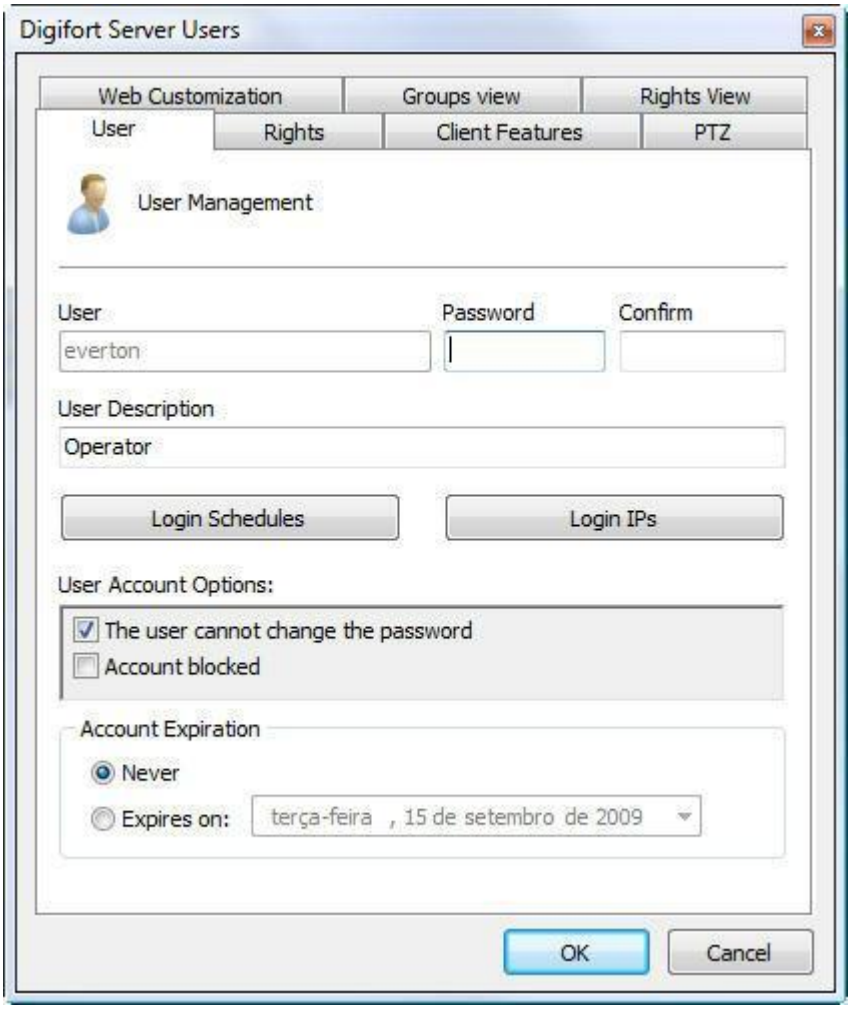
© 2002 - 2011 by Optiview USA all rights

After clicking on the **Add** button, the users editing screen will be opened. Let's start by inserting the user's data, followed by the rights and, lastly, the client features.

To modify a previously registered user, select it and click on **Modify**, and alter the data as explained on the following pages.

To remove a user, select the desired user and click on the **Remove** button.

9.2.1 User data



The first step is to add a User is inform their primary data, they are:

- **User**: Name of the user. This must be informed at login in any module of the Digifort System. After being saved it cannot be modified.
- **Password**: The user's password.
- **Confirm**: Enter the user's password again.
- **Description of the user:** A brief description of the user, for aiding in his identification in the system.
- **User account options**:

© 2002 - 2011 by Optiview USA all rights

- **The user cannot change the password**: With this option marked, the user can never change his password, leaving this up to the system administrator.
- **This user will receive alerts**: With this option marked, the user will receive the configured alerts when some event occurs.
- **Account blocked**: With this option marked, the user will not be able to authenticate himself in the system.

· **Expiration of the account:** In this parameter you can define a date upon which the user account will expire. If the user account expires, he will not be able to authenticate himself in the system. To reactivate an expired account, mark the option Never or change the expiration to a later one.
- **Never**: The user account never expires.
- **Expires on:** The user account expires on the specified date.

Tip

The password can be left blank when registering and the user will be able to register his password during his first access to the system.

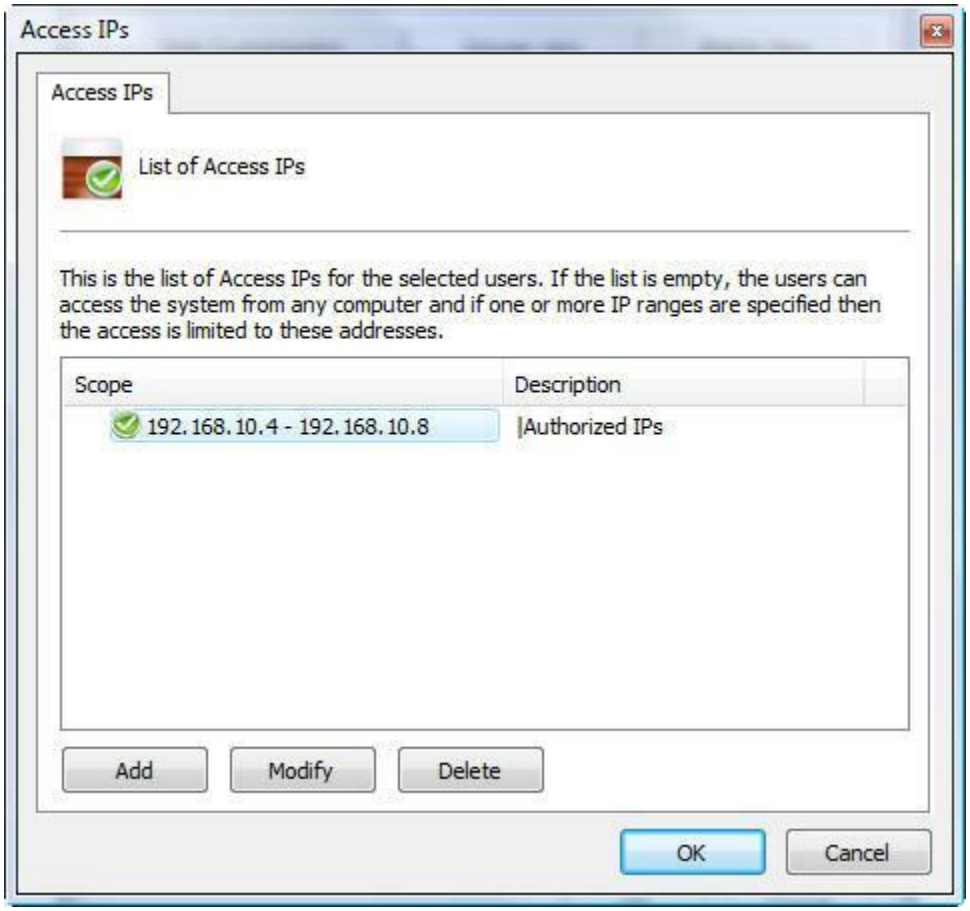
9.2.1.1 Login IPs

The configuration of Login IPs is very important for the security of the Digifort Server, as it is in this configuration that we register the range of IPs that a user can use for his authentication in the system.

For greater security, except in specified cases, it is recommended that the IP of the workstation of the user is registered, blocking access to the system from other locations like, for example, his home.
If this configuration is not done, the user will be able to authenticate at any workstation.

To access this feature, click on the **Login IPs** button, located in the User tab, opening the Login IPs register, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights


Access IPs
Access IPs
List of Access IPs
This is the list of Access IPs for the selected users. If the list is empty, the users can access the system from any computer and if one or more IP ranges are specified then the access is limited to these addresses.
Scope
Description
192.168.10.4 - 192.168.10.8
Authorized IPs
Add
Modify
Delete
OK
Cancel

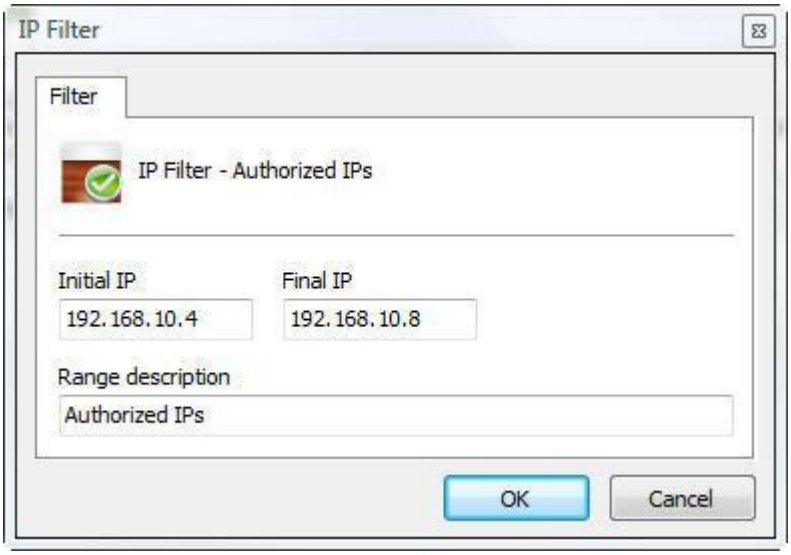
This picture examples a configuration where the user will be able to authenticate himself in the system, using IPs within the range from 192.168.5.2 to 192.168.5.4.

To add an access IP range, click on **Add**. To modify a range of access IPs, select it and click on **Modify**. To exclude a range of access IPs, select it and click on **Exclude**.

9.2.1.1.1 Adding a range of access IPs

To add a range of access IPs, click on Add and the editing screen will be displayed, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



Enter the initial IP and final IP of the range and, lastly, enter a description for the range to be added.

If you wish to add only one IP, fill in the initial IP field and the final IP field with the same value

9.2.1.2 Login hours

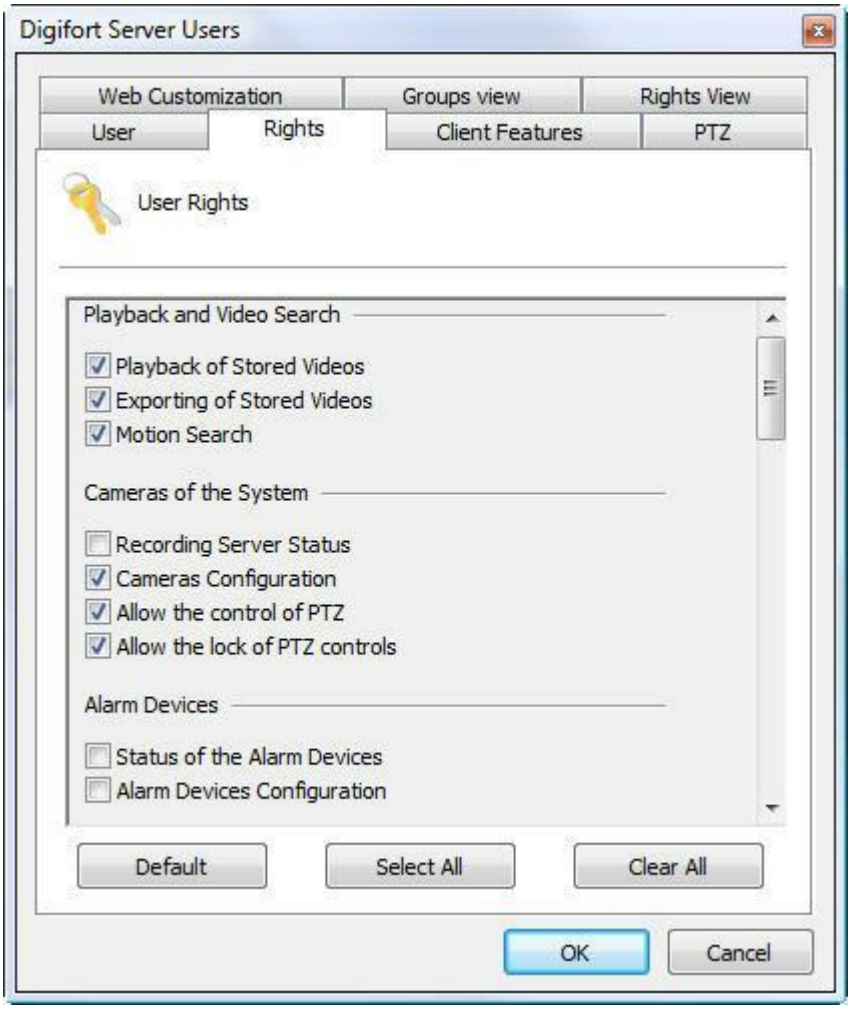
the Digifort server are the login hours, with which it's possible to define the times of day that users can have access to the system.

To access this feature, click on Login Hours, opening the scheduling screen. The function of this screen is specified on page How to configure the scheduling of recording

9.2.2 User rights

After filling in the main user data, the access rights must be configured. As default, the rights are configured for a surveillance user profile, that is, the user will only be able to carry out the system operations of live surveillance and video playback.

© 2002 - 2011 by Optiview USA all rights



- **Playback of stored videos:** Allows the user to visualize previously recorded videos. To learn how to play video back, see the manual of the Surveillance Client.
- · **Exportation of stored videos**: Allows the user to export previously recorded videos for backup or visualization in another workstation. To learn how to export videos, see the manual of the Surveillance Client.
- **Motion search**: Allows the user to carry out motion searches in stored videos. Motion search helps in retrieval of events in a scene. To learn about motion search, consult the manual of the Surveillance Client.
- **Configuration of cameras**: Allows the user to configure the cameras to be managed by the system.
- **Status of the recording server**: Allows the user to check the general status of the system and the individual status of each camera, getting information like used disk space, frames per second received, activity time, etc.
- **Allow PTZ control**: Allows the user to control movable cameras with PTX functions.
- **Allows locking of the PTZ controls**: Allows the user to lock the movement of the camera by priority.
- **Alarm device configurations**: Allows the user to access the configurations of alarm devices.
- **Alarm device status**: Allows the user to access the monitoring of the status of the alarm devices.

© 2002 - 2011 by Optiview USA all rights

- **Alert contacts register**: Allows the user to access the alert contacts register. The contacts must be registered to receive notification of system abnormalities of the occurrence of events.
- **Alert groups register**: Allows the user to access the alert groups register. Alert groups have the purpose of grouping alert contacts aimed and categorizing and sending notifications to various contacts.
- **Alert log configurations**: Allows the user to access the configurations of the alert logs. Alert logs register all alerts that occur in the system such as the setting off of a siren, for example.
- **Alert log visualization**: Allows the user to visualize the alert logs.
- **Permit activation of manual events**: Allows the user to activate miscellaneous manual events like, for example, a siren via Digifort.
- **Server configurations**: Allows the user to modify the system's global configurations, such as limit of connections with the server, limits of recording in disk, etc.
- **IP Filters**: Allows the user to access the IP filters.
- **Server information**: Allows the user to check information about the functioning of the server, getting information such as network input and output traffic.
- **Server licences**: Allows the user to access the server licenses configurations.
- **Server log configuration**: Allows the user to access the server log configurations. Among other things, these logs register system errors and user actions in the system.
- **Visualization of server logs**: Allows the user to access the configurations of the server logs.
- **Surveillance screenstyles**: Allows the user to create his own surveillance screenstyles.
- **Web server configuration**: Allows the user to access the configurations of the Web server. The Web server Web makes it possible to carry out surveillance of cameras and alarms via any Internet navigator.
- **User register**: Allows the user to access the user register.
- **User activity in the server:** Allows the user to monitor the activity of the users in the server. To learn how to use this feature, see . Monitoring user activity

Tip

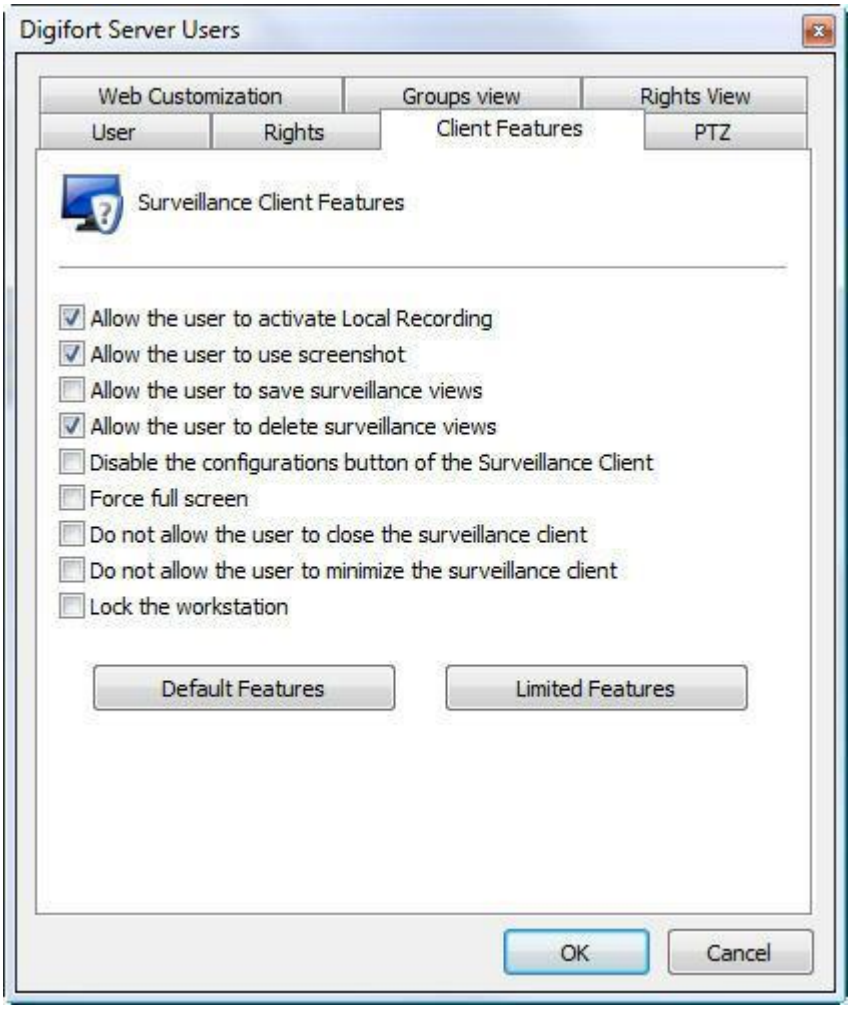
User rights are categorized in the same order as the Configurations Menu.

9.2.3 Surveillance Client Features

The configuration of the features of the Surveillance Client is very important for the security of a site. This feature offers tools that affect the person who monitors the cameras, causing other factors to impair the attention of the operator.

To access these tools, click on **Client features.**

© 2002 - 2011 by Optiview USA all rights

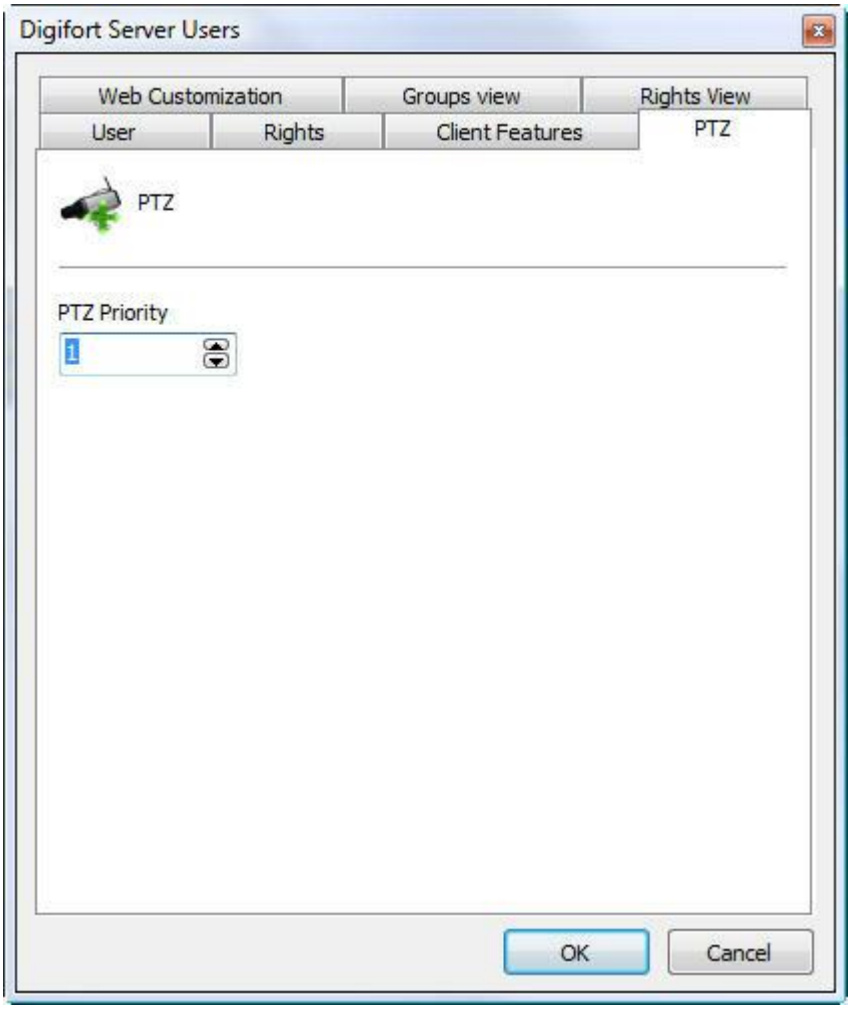


- **Allow the user to save surveillance views**: Allows the user to create his surveillance views. To learn more about the creation of surveillance views, consult the manual of the Surveillance Client.
- **Allow the user to eliminate surveillance views**: Allows the user to eliminate surveillance views.
- **Disable the configurations button on the surveillance client**: Blocks user access to the configurations of the surveillance client. To learn about the configurations of the Surveillance Client, consult the manual of the Surveillance Client.
- **Don't allow the user to close the surveillance client**: Blocks closing of the Surveillance Client by the user.
- **Don't allow the user to minimize the surveillance client**: Blocks minimization of the Surveillance Client by the user, keeping it locked to the system.
- **Blocks the workstation**: Blocks the user's workstation, not allowing the use of functions such as CTRL + ALT + DEL, ALT + TAB, and any other command that could terminate the Surveillance Client.

9.2.4 PTZ

These configurations allow the definition of a priority for the user in PTZ control for the cameras.

© 2002 - 2011 by Optiview USA all rights



The priority with value 1 is the highest of all. Thus, no user with priority equal or lower can unlock the PTZ while this user is using it.

Now let's imagine a user with priority 3. This user loses control of PTZ to another with higher priority, in the case 1 or 2, but no user on the same level or lower (3,4,5,6...) will be able to take control of the PTZ while it's being used.

9.2.5 Web Customization

These configurations allow customization of the page of interaction with the user when Digifort is accessed by way of an Internet navigator.

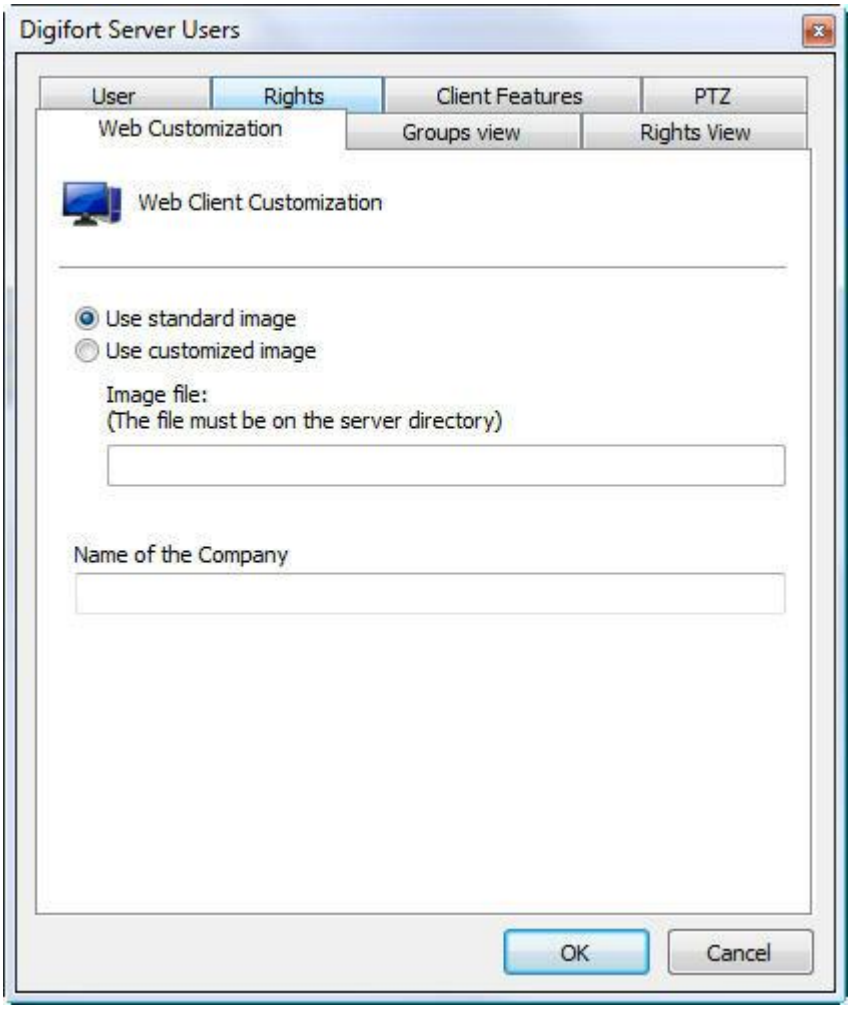
This feature can be used for customizing the page of interaction with the user showing the company's logo, for example.

A different web customization can be created for each user, by simply specifying these parameters in the correct way in each user's register.

To access these configurations, click on the **Web Customization** tab, as shown in the

© 2002 - 2011 by Optiview USA all rights

picture below:

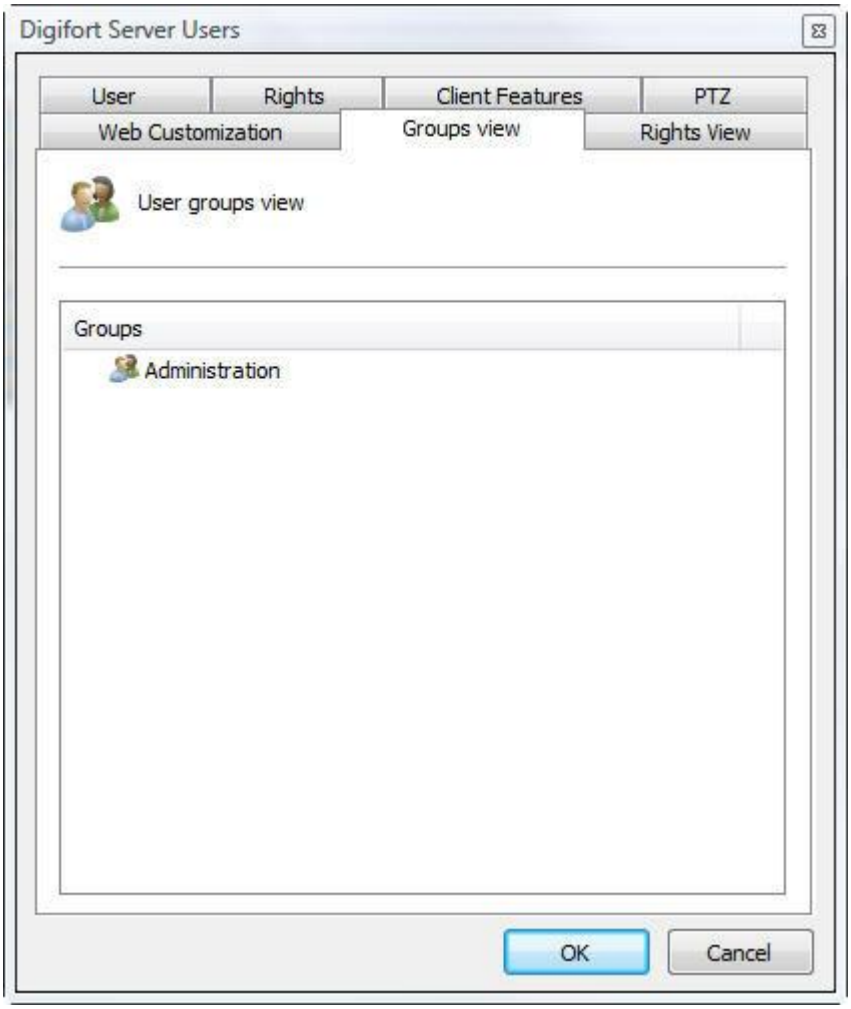


- **Use default image:** Displays the Digifort logo on the page of interaction with the user.
- **Use customized image**: Enables the path field for the image allowing for localization of an image in the computer which will be used on the page of interaction with the user, substituting the Digifort logo.
- **Name of the company:** Enter the name of the company to be shown on the page of interaction with the user.

9.2.6 Groups Inquiry

Allows viewing of the groups in which the user is registered.

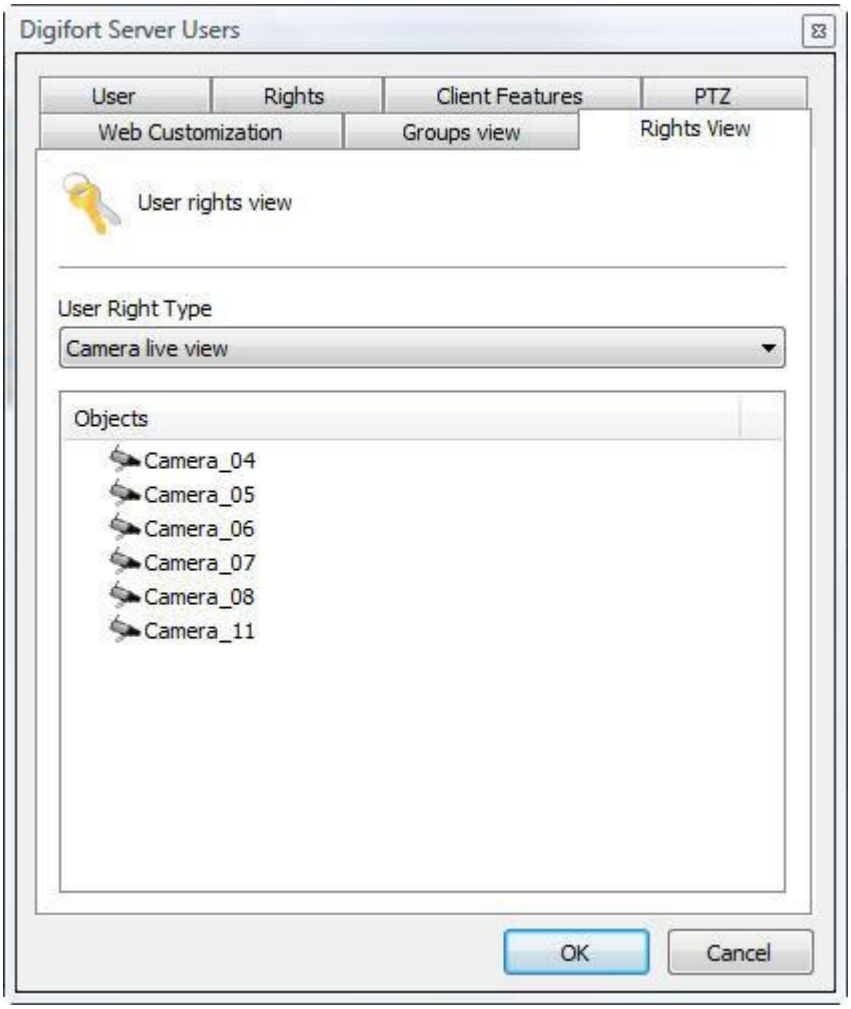
© 2002 - 2011 by Optiview USA all rights



9.2.7 Rights Inquiry

This screen allows viewing of the rights given to the user, such as, for example, the right to view and playback cameras and maps.

© 2002 - 2011 by Optiview USA all rights



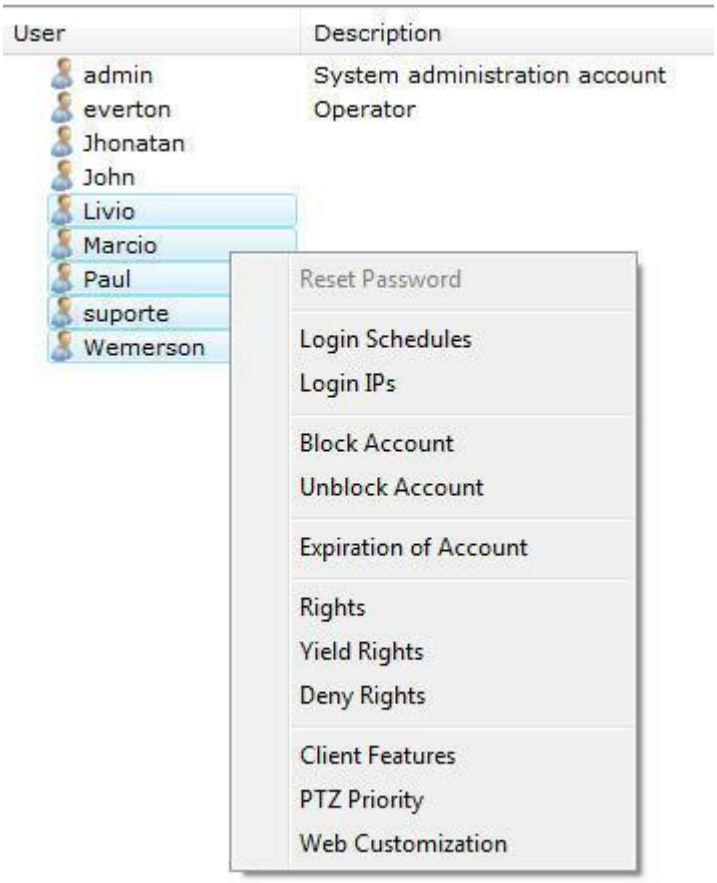
This screen offers the following functions:

- **Type of right**: List of the types of rights given to the user.
- **Objects:** List of the objects related to the given right

9.3 User administration functions

The Digifort's User Administrator offers rapid access to the most common user configurations. In the user register, select the desired user and click on the right button. A menu will be opened, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



9.3.1 Reset password

Resets the password of the selected user, leaving it blank. For security reasons, this option will be available selecting one user at a time.

9.3.2 Login IPs

Opens the configurations of user login IPs. This configuration allows you to define from which IPs a user can authenticate himself in the system. To learn how to use this feature, see Login IPs

9.3.3 Block account

Blocks the account of selected users, making them unable to authenticate in the system. com que eles não consigam autenticação no sistema.

9.3.4 Unblock account

Unblocks the account of selected users, making them able to use the system again.

© 2002 - 2011 by Optiview USA all rights

9.3.5 Account expiration

Defines an expiration date for the accounts of the selected users. After the expiration date, the user can no longer authenticate himself in the system..

9.3.6 Rights

Opens the user rights screen. To learn about user rights, see Login hours

9.3.7 Give rights

Opens the user rights screen giving the selected rights. If no right is selected, but some user has it, the rights defined here will be added. somados.

9.3.8 Deny rights

Opens the user rights screen denying the selected rights.

9.3.9 Features

Opens the features screen of the Surveillance Client. To learn about this feature, see Surveillance Client Features.

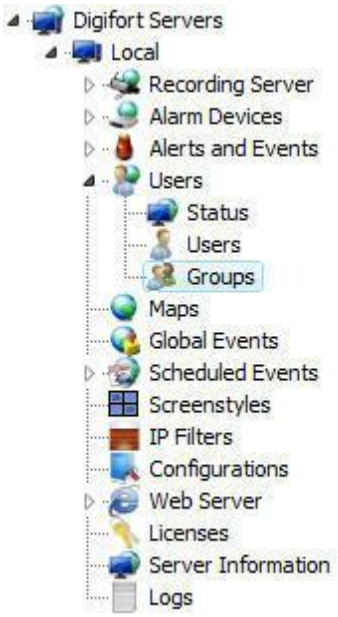
9.3.10 Web customization

Opens the screen for configuration of the user's web customization. To learn how to use this feature, see Web Customization

9.4 Adding, altering and excluding Groups

To access the group management feature, locate Groups in User in the server's Configurations menu as shown in the picture below:

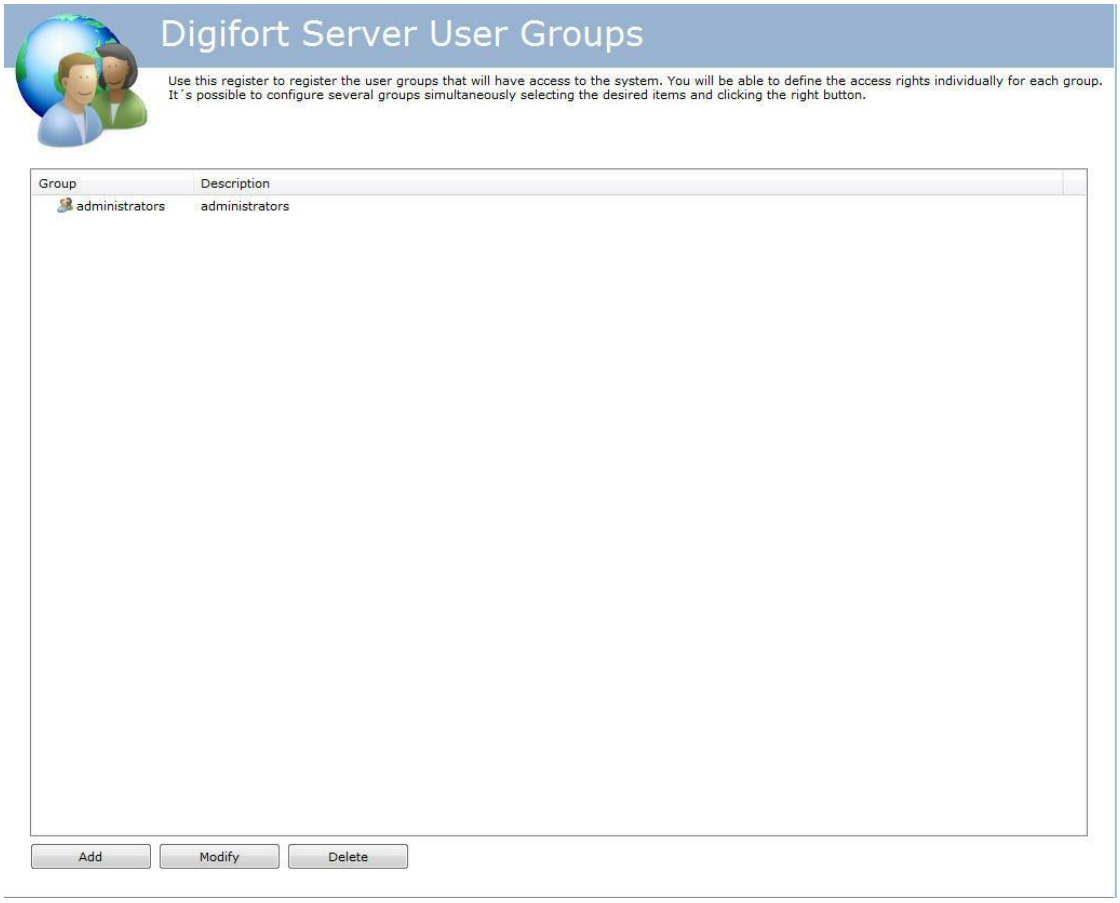
© 2002 - 2011 by Optiview USA all rights



The ‘Groups’ option was created to facilitate user management within the system.

Once this is done, the Groups management screen will open on the right as illustrated in the picture below:

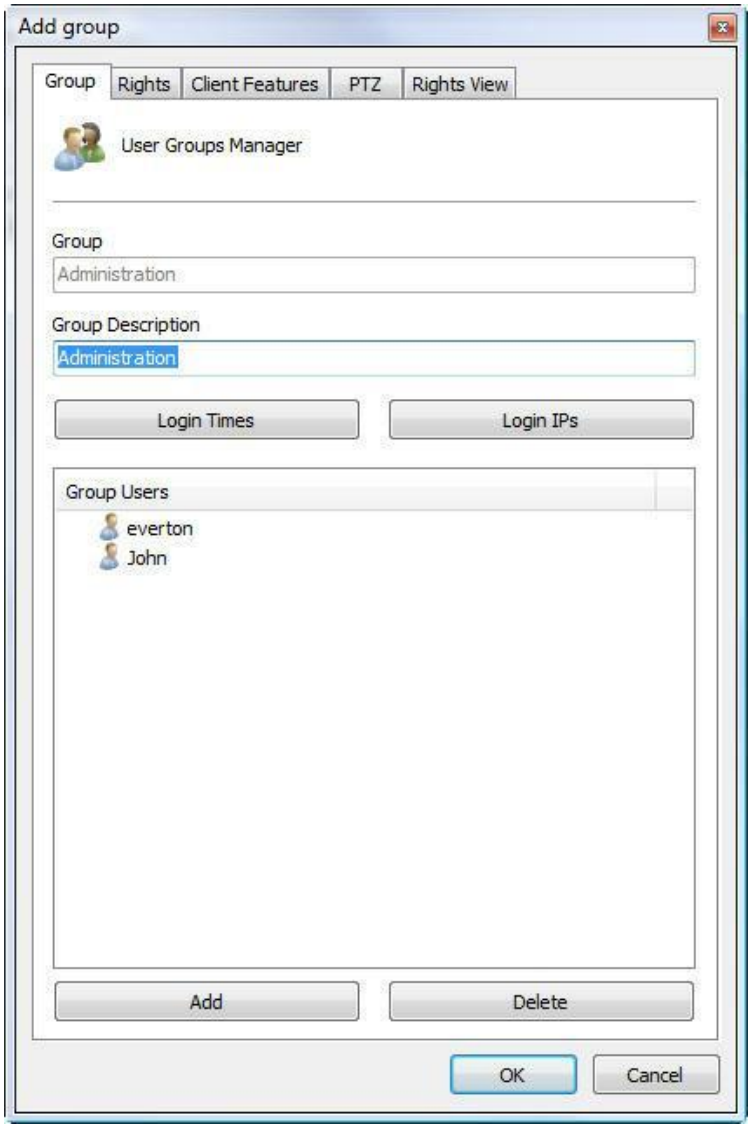
© 2002 - 2011 by Optiview USA all rights


Digifort Server User Groups
Use this register to register the user groups that will have access to the system. You will be able to define the access rights individually for each group.
It´s possible to configure several groups simultaneously selecting the desired items and clicking the right button.
Group
Description
administrators
administrators
Add
Modify
Delete

By clicking on the Add button, the group edition screen will open up. Let's start by introducing a group, moving on to the entitlements and then the features.

To change an already registered user, select it and click on Change and then change the data as explained throughout the manual.
To remove a user, select the user you wish to remove and click on the Remove button.

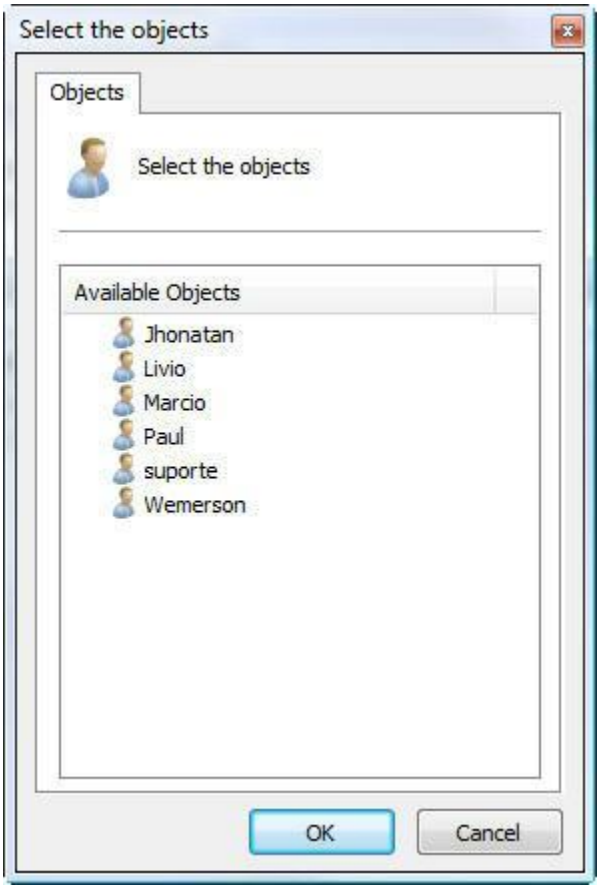
© 2002 - 2011 by Optiview USA all rights



When adding a group, the first step is to indicate its main data, i.e.:

- Group: Username, which must be indicated when logging in to any module of the Digifort System. Once saved it cannot be altered.
- Group description: A brief description of the user to help identify him in the system.
- Login times**:** To learn about this feature refer to Login Times
- Login IPs: To learn about this feature refer to Login IPs
- Group Users: List of users in the group. To add a user to the group, simply click on **Add** and a window will open so that you may select the user to be added as shown in the picture. To remove a user, simply select it from the list and click on the **Remove** button.

© 2002 - 2011 by Optiview USA all rights



9.4.1 Group rights

After filling in the main user data, the access rights must be configured. As default, the rights are configured for a surveillance user profile, that is, the user will only be able to carry out the system operations of live surveillance and video playback.

As configurações de direitos para o grupo é igual a configuração de direitos de usuário.

9.4.2 Surveillance Client Features

The configuration of the features of the Surveillance Client is very important for the security of a site. This feature offers tools that affect the person who monitors the cameras, causing other factors to impair the attention of the operator.

The configuration of the Resources of the Surveillance Client for the group is the same as the configuration of the Resources of the Surveillance Client of the user. To learn how to configure the Resources of the Surveillance Client of the group see Surveillance Client Features.

© 2002 - 2011 by Optiview USA all rights

9.4.3 PTZ

These configurations allow the definition of a priority to the group of or PTZ control of the cameras.

The configuration of the PTZ for the group is the same as the configuration of the PTZ of the user. To learn how to configure the PTZ of the group see PTZ

9.4.4 Rights Inquiry

This screen allows the viewing of the rights given to the group, such as, for examplo, the right of viewing and playback of cameras and maps.

The configuration of the Rights Inquiry for the group is the same as the configuration of the Rights Inquiry of the user. To learn how to configure the Rights Inquiry of the group see Rights Inquiry

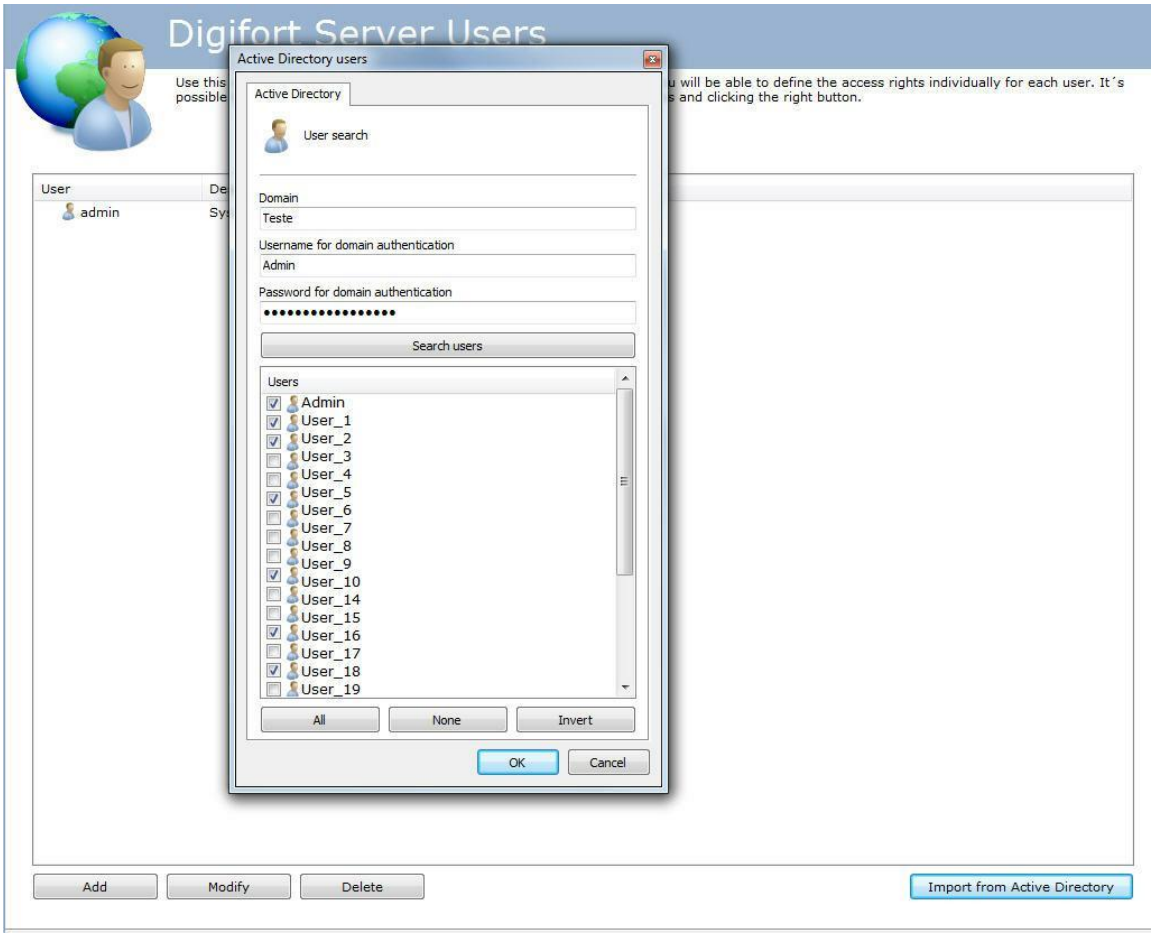
9.5 Integration with the Active Directory

The **Active Directory** is a set of archives located in the domain server which holds all the information needed to control user access to the network. The usernames and passwords are registered in the Active Directory, including authorizations to access archives, printers and other network features, the disk quotas, computers and times each user can use, etc.

Interaction with the Active Directory means that network users of the Digifort server domain can be imported and integrated as Digifort users.

There are 2 ways in which to integrate them: the first is to import the users directly from the Active Directory. To do so, in Users click on **Import** from **Active Directory** as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



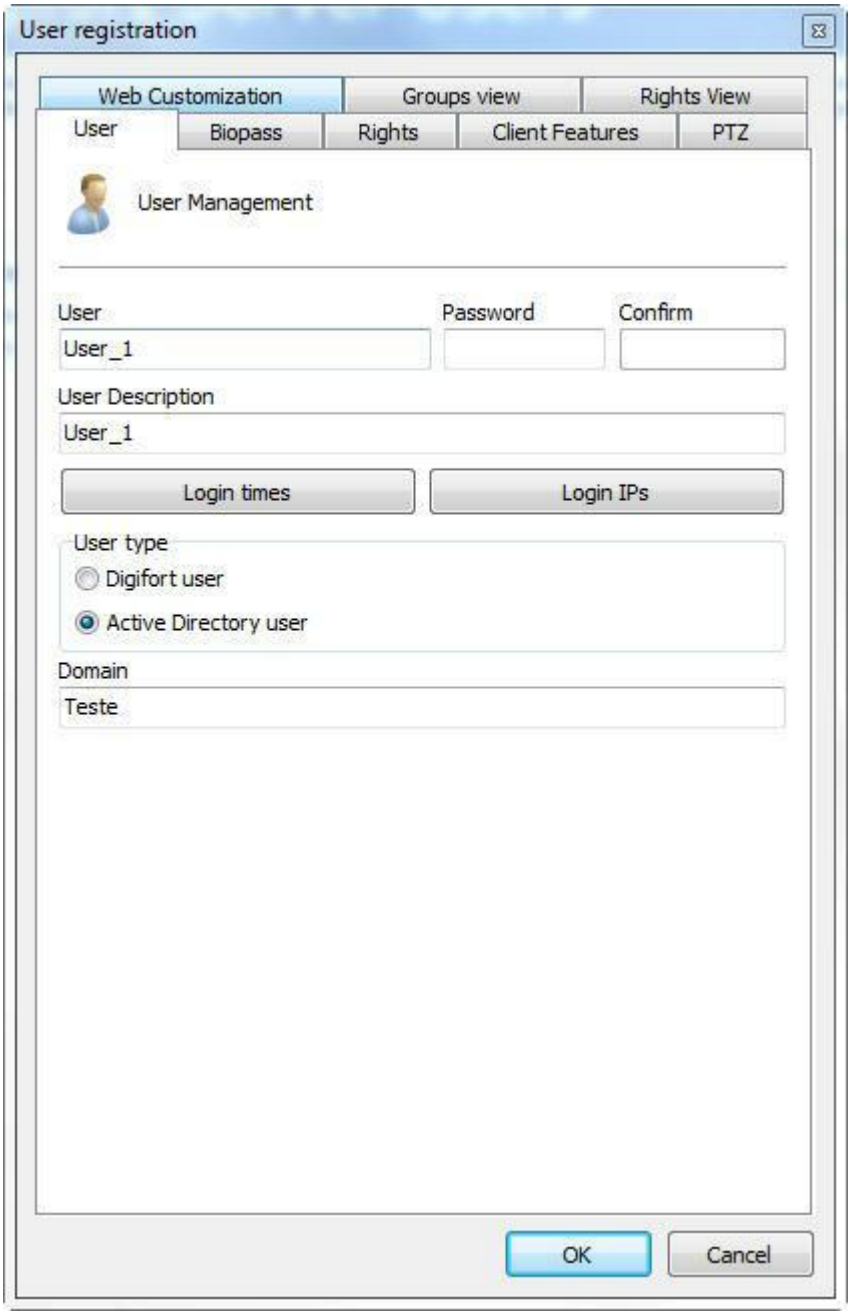
This screen has the following functionalities:

Domain: Type the network domain.
Username for domain authentication: Username to be authenticated in the domain.
Password for domain authentication: Domain user password.

After filling in each field, click on **Search Users** and all users registered in the domain will be listed. To add users to Digifort simply select them and click on OK.

A user belonging to the domain has the following configuration screen:

© 2002 - 2011 by Optiview USA all rights



All the username and password options are blocked because the authentication is made in the domain and no longer in Digifort, so the block account options, Biopass and account Expiry will no longer be available.

It is possible to change a user already found in Digifort to a network user, simply change the "User Type" field. To function properly, the username and the domain must be filled in correctly according to the users registered in the current Domain.

© 2002 - 2011 by Optiview USA all rights

Chapter



10 BioPass

BioPass is an authentication product via Digifort's biometry. To increase the security of users who have been authenticated in the system, it is possible to enforce a biometric authentication.

10.1 How to install BioPass on your computer

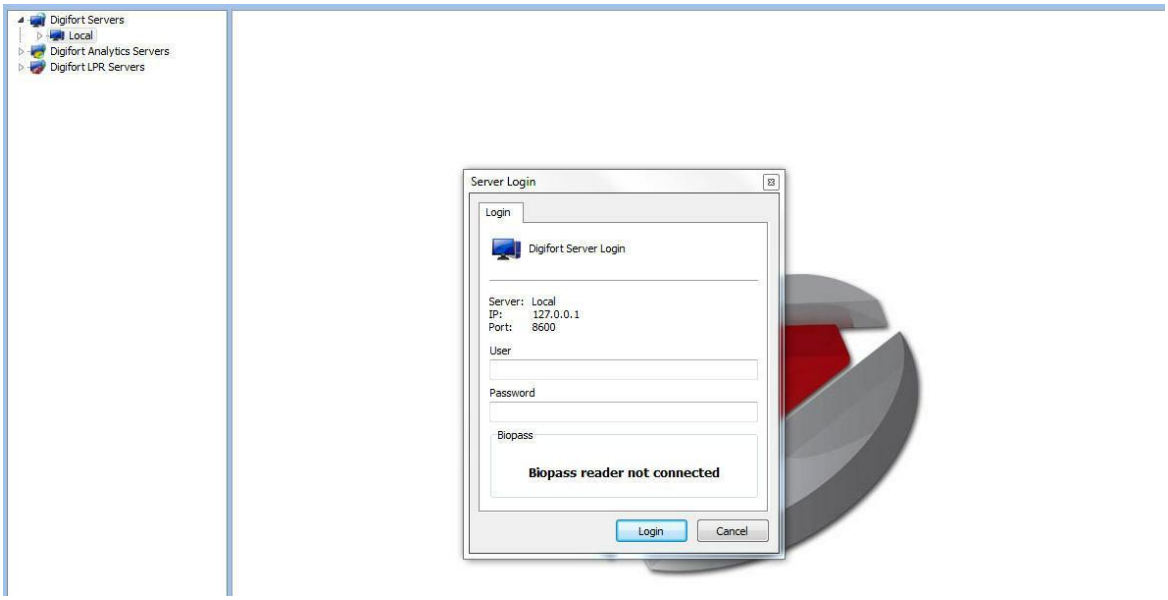
After installing the Digifort 6.4.0.0 Enterprise, , the drivers of the BioPass Digital Reader will be available to be installed by the operational system.
With the 6.4.0.0 Enterprise already installed, connect the BioPass reader to your computer and the following message will show up on the Operative System:



Once this message is shown, you can configure the BioPass in Digifort.

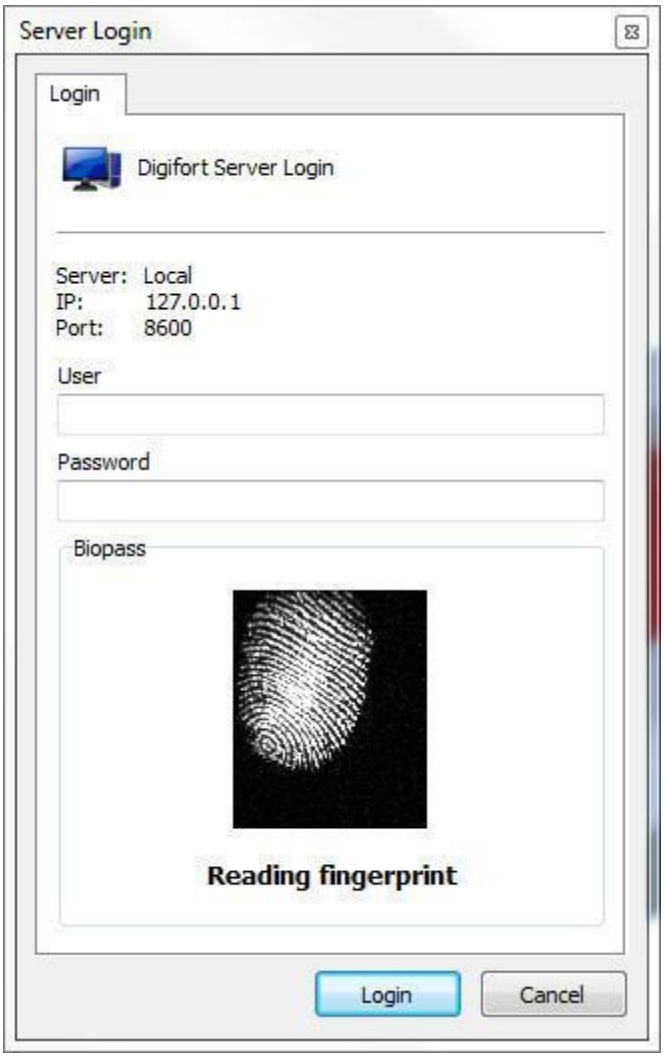
10.2 How to configure the BioPass

If the reader is not recognized or is not plugged in, the message **Biopass reader not connected** will show up as in the picture below:



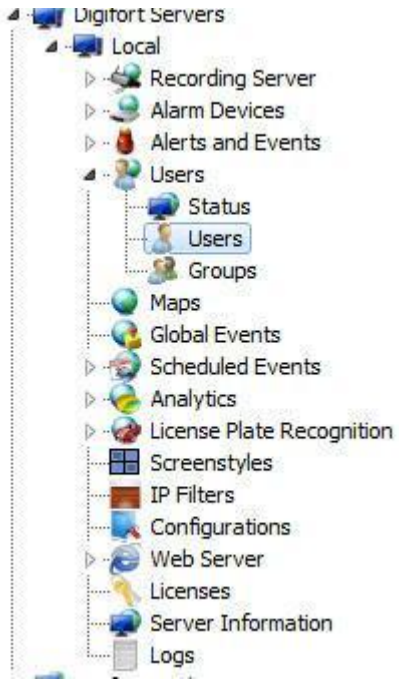
© 2002 - 2011 by Optiview USA all rights

Once the reader is plugged in and recognized by the operative system, open Digifort's Administration Client and Log into your server.
Note that the Login screen now has a differential as shown in the picture below:



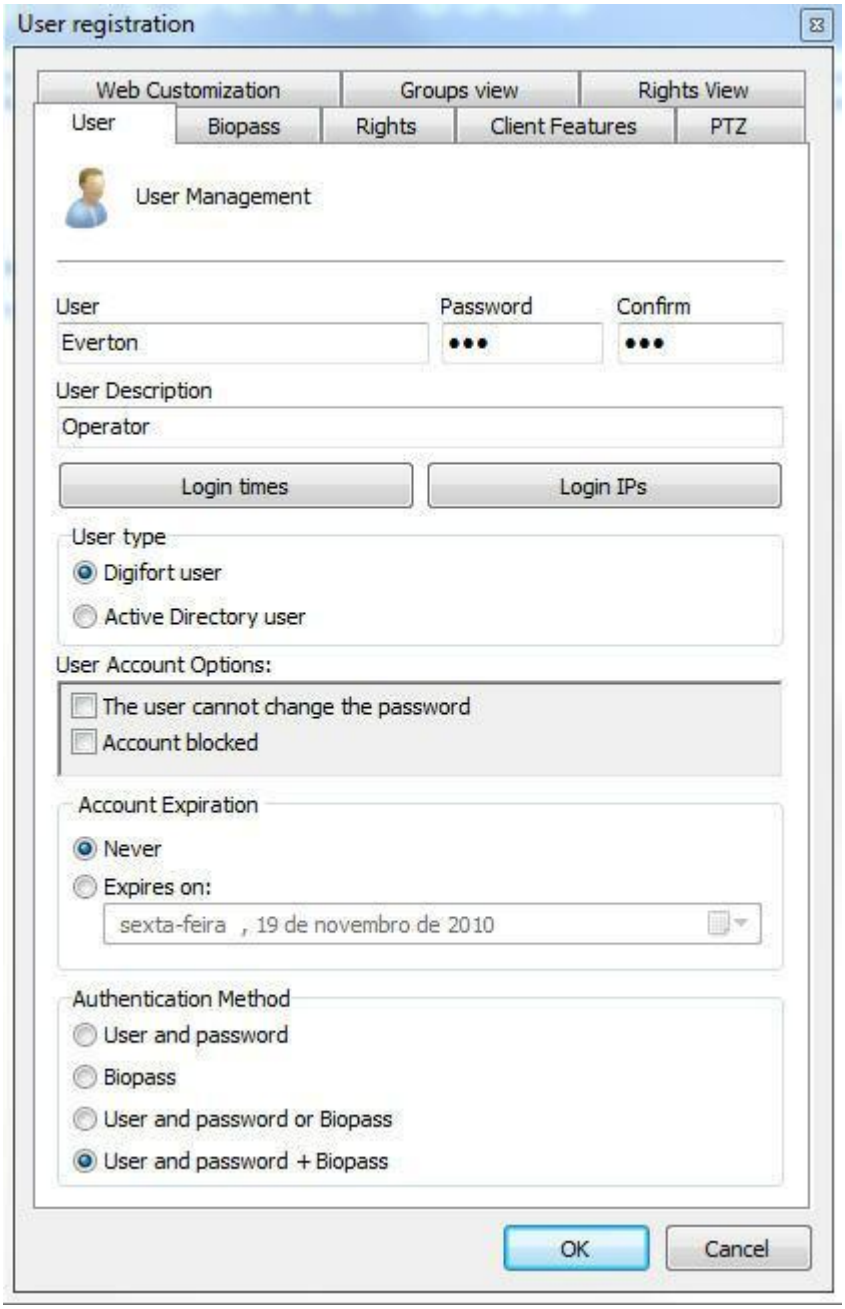
There is a finger print view on the screen but no finger print has yet been registered, so the Login must be made with the username and password.
Now, to configure the finger prints go to "**Users"** as shown in the following picture:

© 2002 - 2011 by Optiview USA all rights



Now, create a user to configure the Biometric Reader. (See User Management to learn about the system's users):

© 2002 - 2011 by Optiview USA all rights



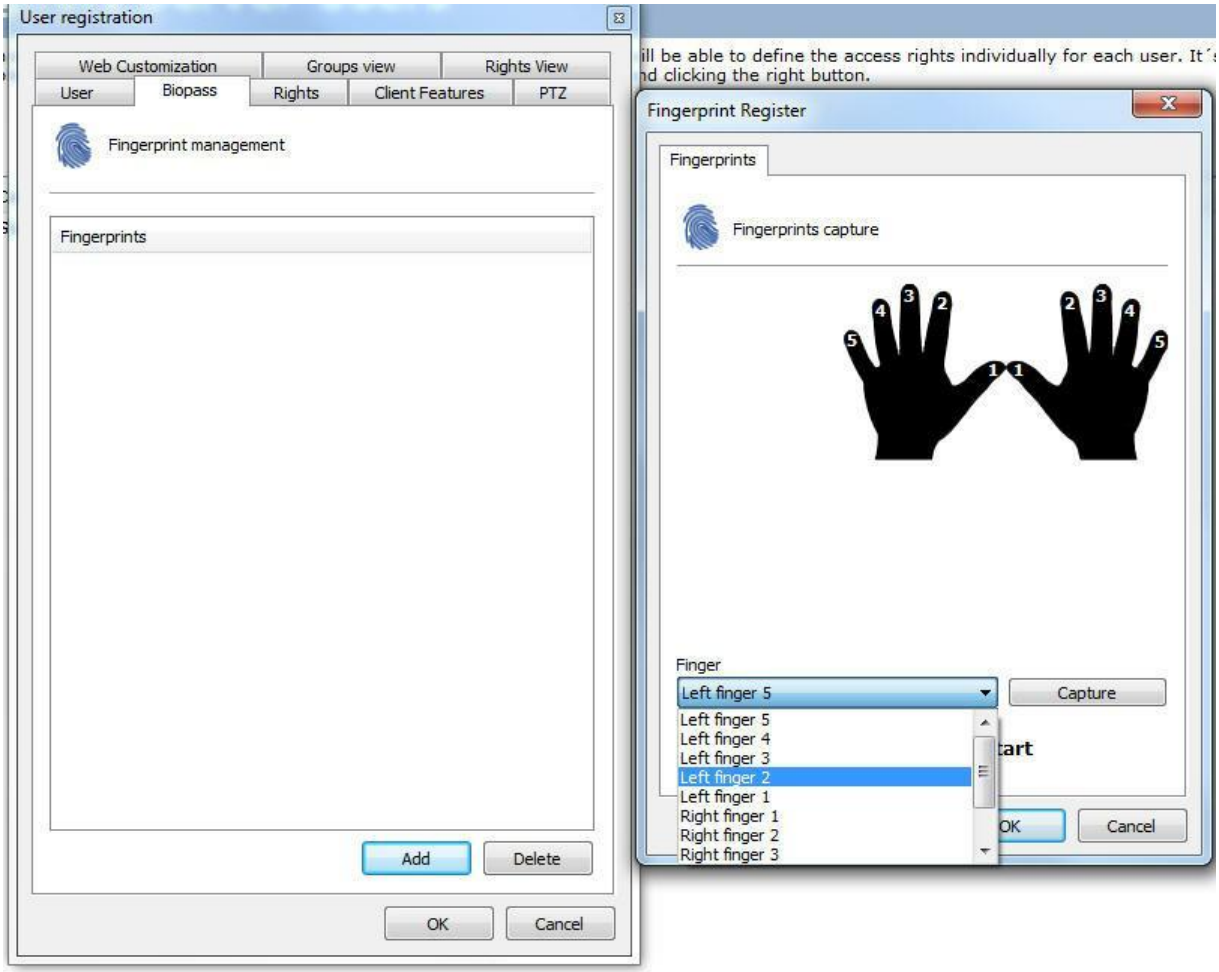
Insert a username, a password and a description for the New User. In the field "**Authentication Method**" there are four options:

- Username and password: System's standard authentication.
- **Biopass:** Only asks for the finger print authentication
- **Username and password or BioPass**: The login can be made with the username and password or BioPass. (Not recommended unless you need to use the web server as it does not have the BioPass functionality).
- Username and password + Biopass: Needs username and password + Biopass for login.

© 2002 - 2011 by Optiview USA all rights

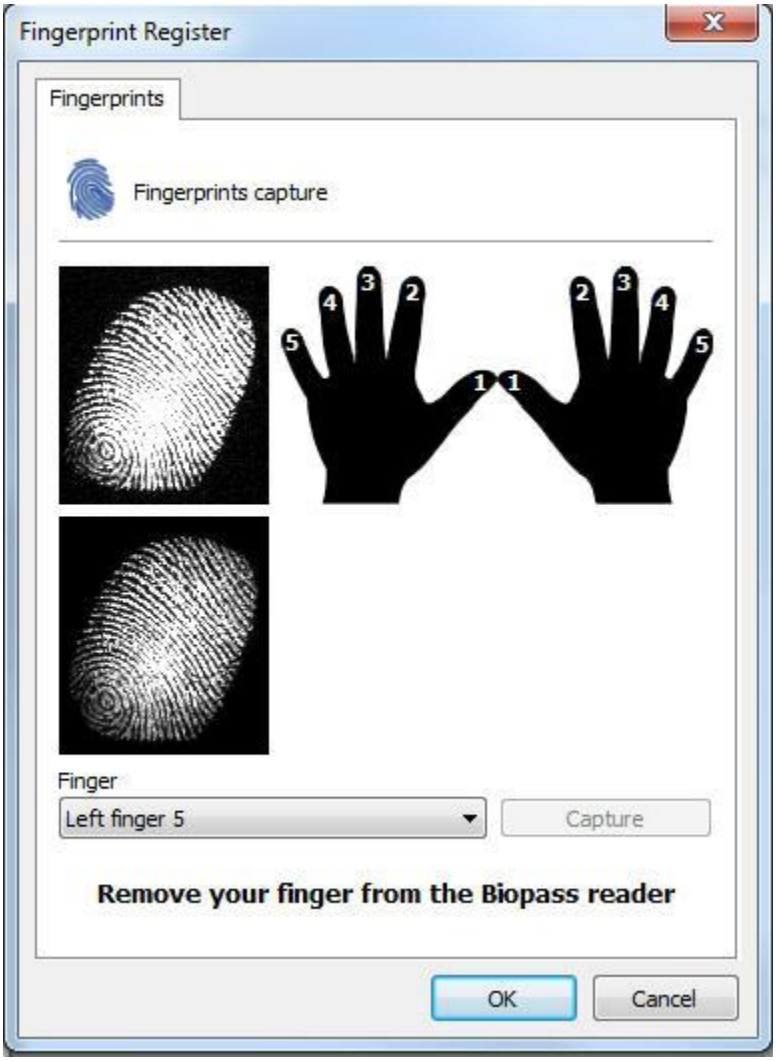
Here the user selects how he will log into the system, in this case **"Username and Password + Biopass".**

Remember that the option "User and Password + Biopass" is the most recommended in terms of security as it will force the user to use his username and password and also use the biometric authentication.
Now this part has been configured, we can open the **"BioPass"** tab as shown in the following picture:



Click on "**Add"** and, on the screen on the right select the finger you will be using for the digital print (you can also click on the number on the 'hand' picture). Once you have decided which print to use click on "Capture"

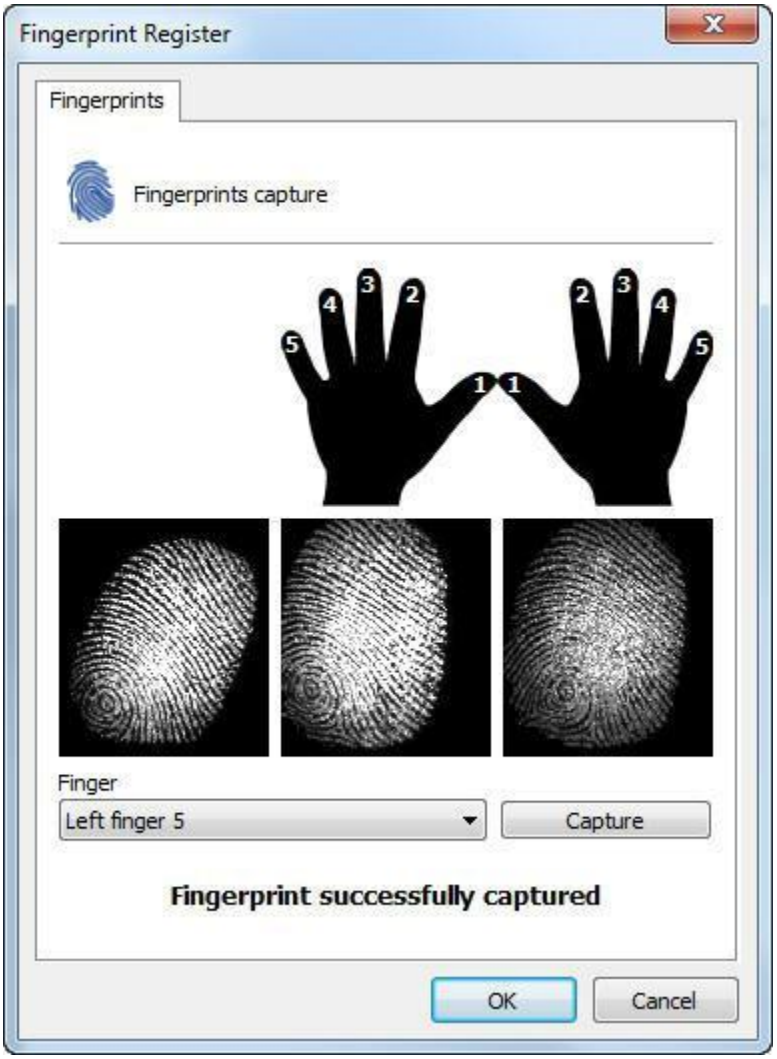
© 2002 - 2011 by Optiview USA all rights



A minor change has occurred on the screen and you should now see the instructions to configure the Digital authentication.
The software will ask you to capture three digital prints of the same finger. Place your finger on the BioPass and remove it when the message **Remove your finger from the BioPass** reader is shown.

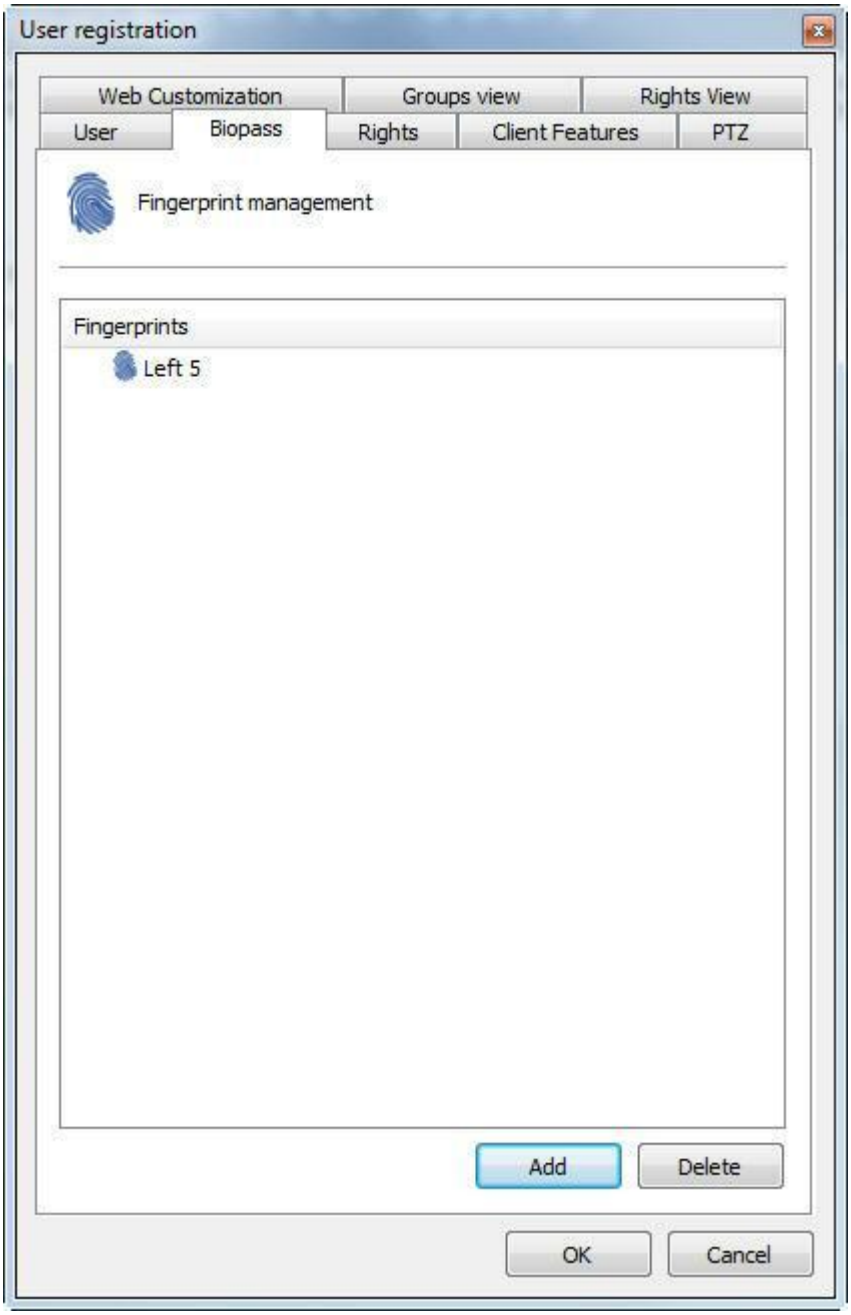
Once the print has been captured, you should receive the message **Digital print captured successfully:**

© 2002 - 2011 by Optiview USA all rights



When finished, click on “OK” to save the configuration applied to that print and you will see a screen with the captured finger prints as in the picture below:

© 2002 - 2011 by Optiview USA all rights



For security purposes, it is recommended that you capture more than one finger.
From now on, the login can be made via BioPass both in the Administration Client as well as the Surveillance Client.

© 2002 - 2011 by Optiview USA all rights

Chapter



11 Maps

The Digifort software brings another built-in feature – a synoptic map, which makes the complete surveillance of an industrial plant, a building, etc., possible. With the map there is better viewing and control of the site, making the viewing of cameras as well as activation of alarms possible.

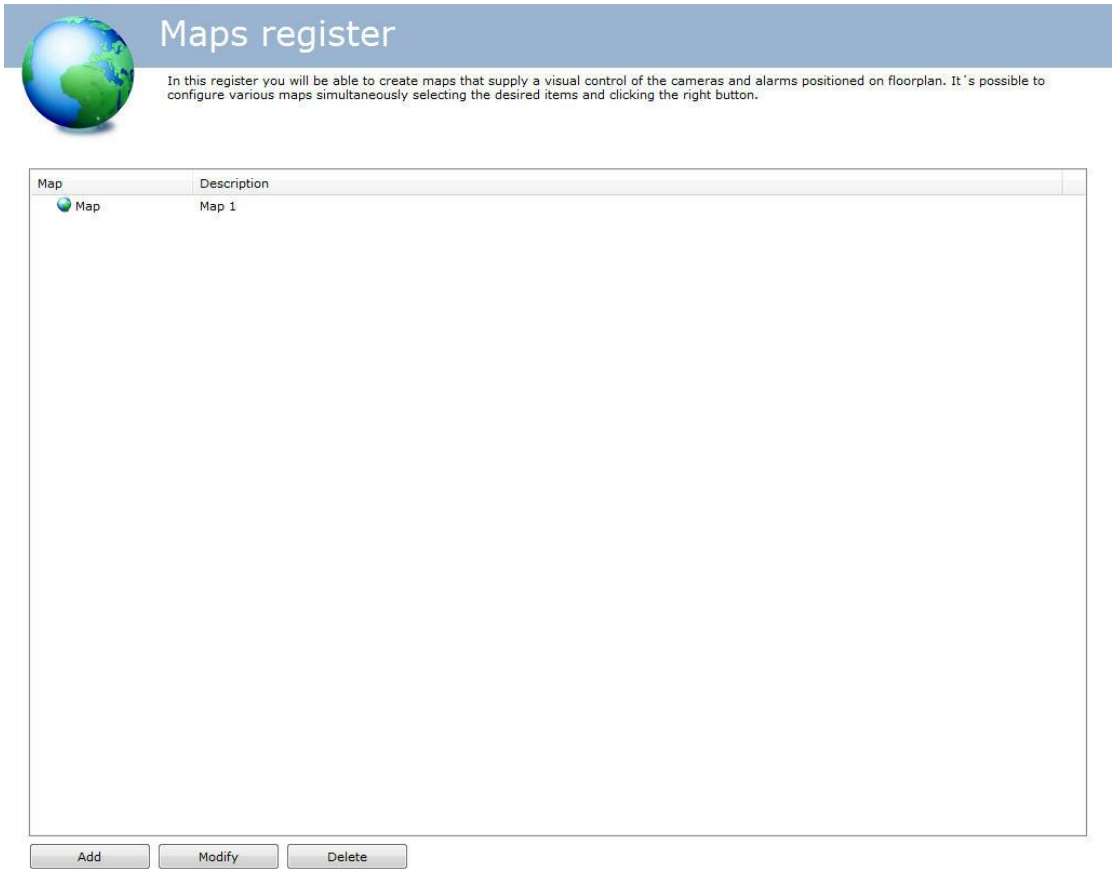
11.1 Registration of Maps

To register a map, click on the item Maps in the Configurations Menu, as shown in Figure bellow:



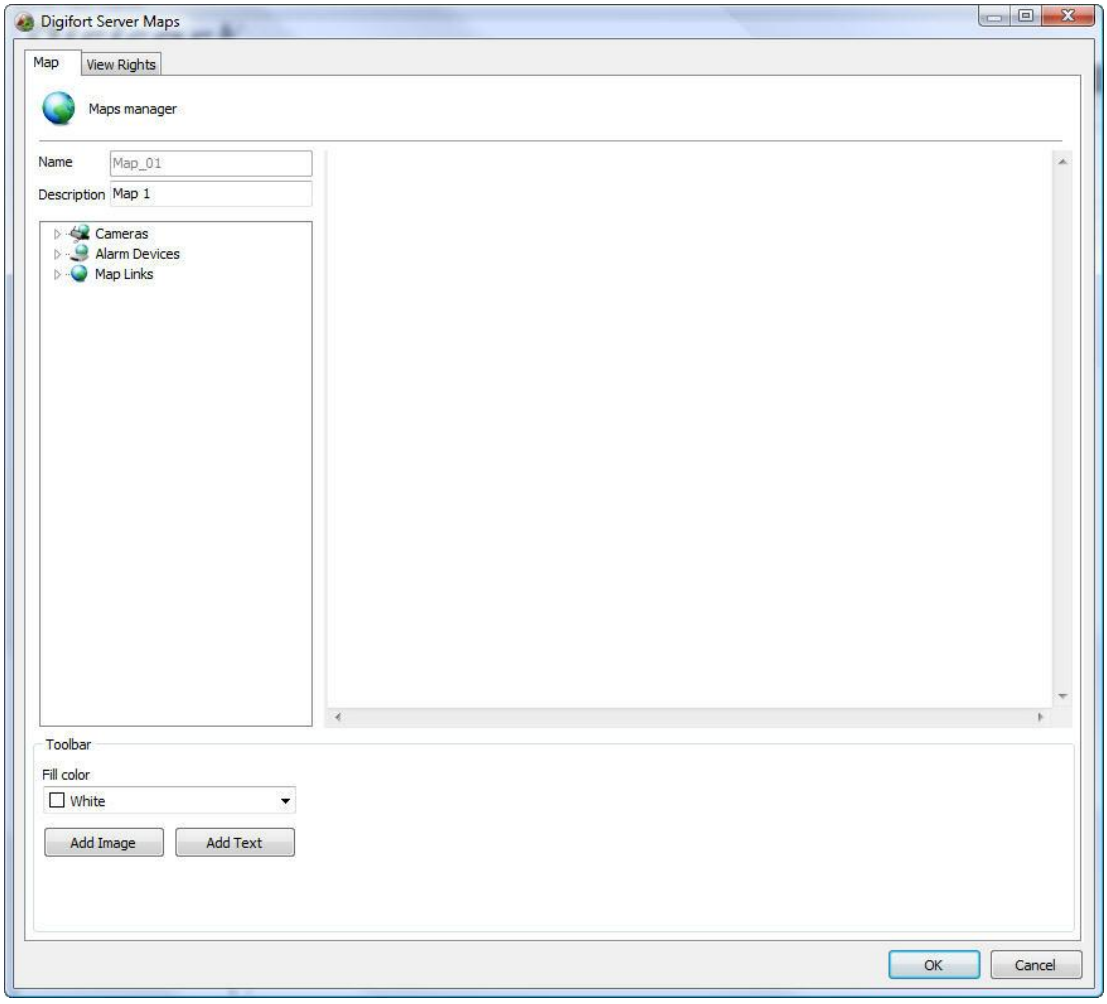
Once this is done, the system's map registration screen will be opened up on the right side, as shown in Figure bellow:

© 2002 - 2011 by Optiview USA all rights


Maps register
In this register you will be able to create maps that supply a visual control of the cameras and alarms positioned on floorplan. It´s possible to configure various maps simultaneously selecting the desired items and clicking the right button.
Map
Description
Map
Map 1
Add
Modify
Delete

Click on Add to open the map configurations screen, as shown in Figure bellow:

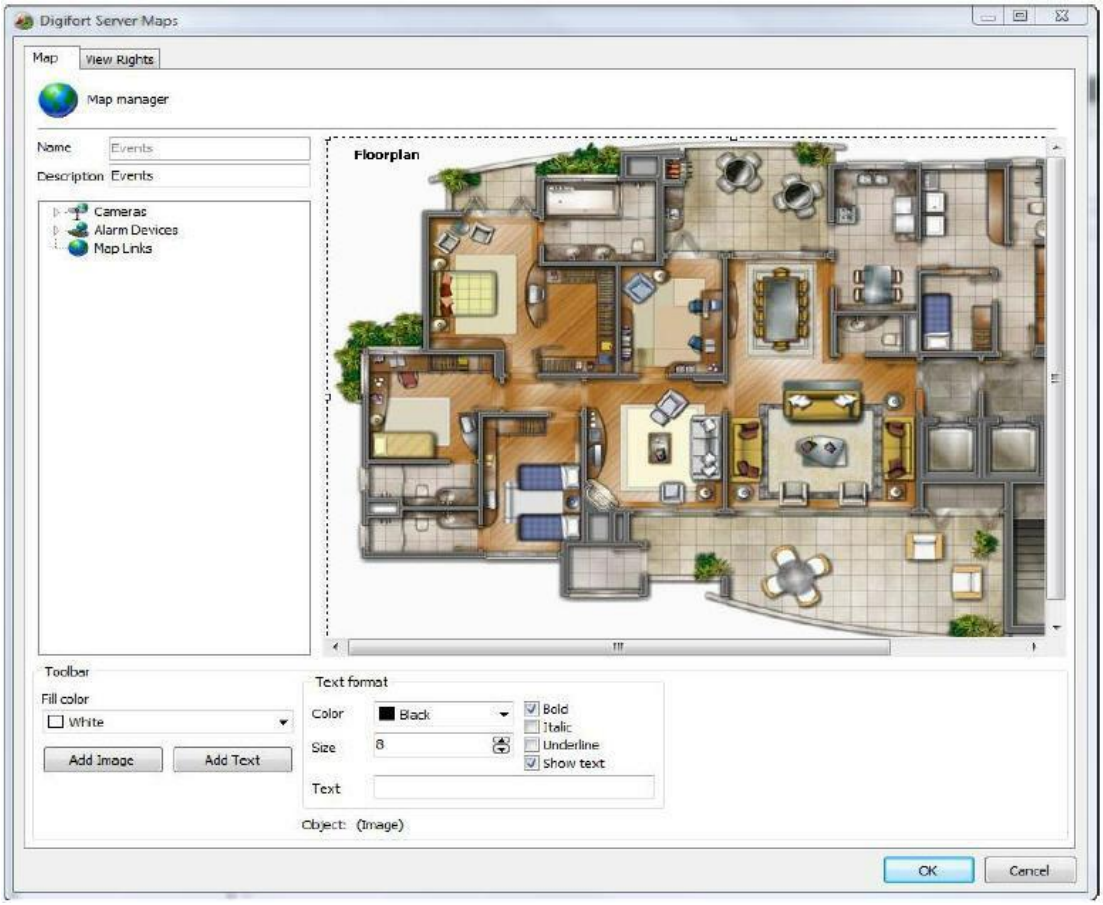
© 2002 - 2011 by Optiview USA all rights



Click on **add** image to locate the desired figure for your map. The system supports images in jpg and jpeg format.

Once the image is chosen, it Will be displayed in the Center of the screen as shown in Figure bellow

© 2002 - 2011 by Optiview USA all rights

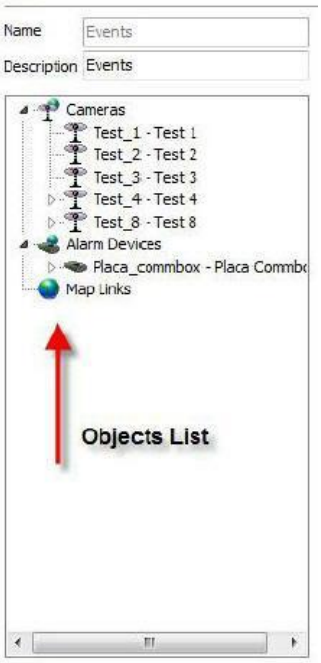


With the button **Add text**, captions can be added to the map. Once created, the text and its font can be edited. Simply select it and change the properties of **Text formatting** found in the lower part of the screen.
These option are valid for any text object of the map:

- **Color**: Changes the color of the text.
- **Size**: Changes the size of the text.
- **Text**: Changes the text of the caption.
- **Bold**: Leaves the text in bold-face letters.
- **Italics**: Leaves the text in italic letters
- **Underline**: Underlines the text.
- **Show text**: Shows or doesn't show the text in an object.

To position the objects in the map simply drag it from the list the left of the screen as the figure shows.

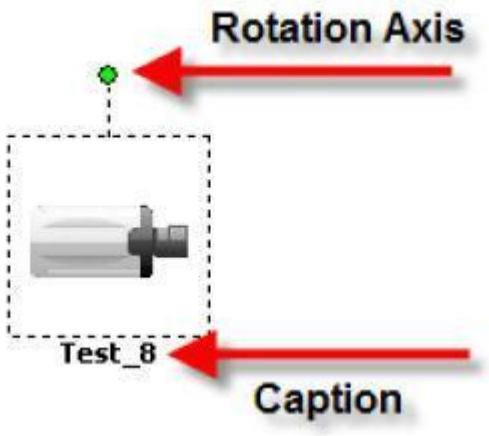
© 2002 - 2011 by Optiview USA all rights



11.1.1 Adding Cameras

In the list of cameras located at the left drag the desired camera to the map. It takes the form of a camera on the map as shown in Figure bellow.

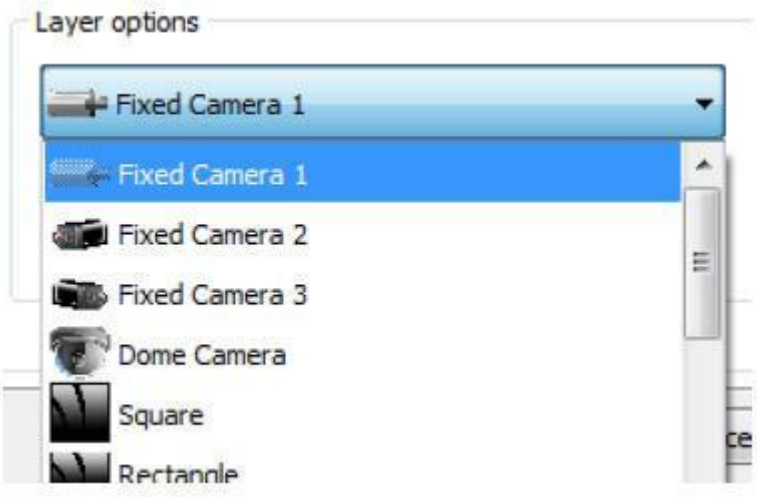
To move it above the map, simply click on its icon and drag it to the desired location.



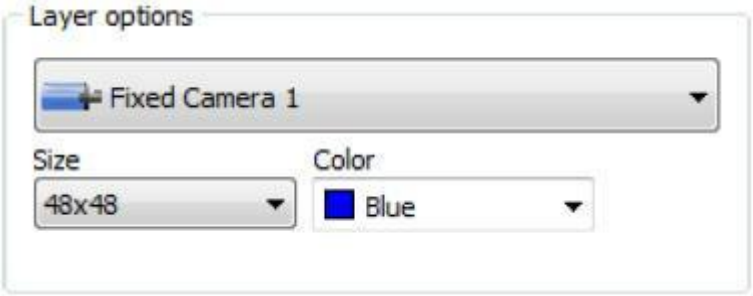
The camera can be rotated by the rotation axis demonstrated in the figure. Simply click on it and move the o cursor of the mouse.
The configurations for the caption of the camera obey the same rule on page.

It's possible to change the icon of the camera. Select it and in the **Layer Options** Menu, choose the desired icon as demonstrated in Figure bellow:

© 2002 - 2011 by Optiview USA all rights



There is also an option for changing the size and color of the icons. In the **Layer options** menu locate the **Size** and **Color** shown in the figure and change the values clicking on them.

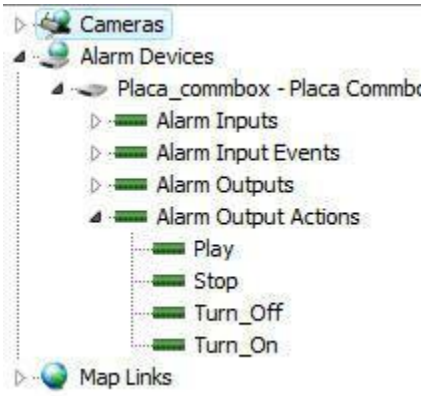


11.1.2 Adding Functions to the Alarm Board

With the events already configured on the alarm board, it's possible to add them for rapid access by way of the map. To learn how to configure events of the board, see How to configure the I/O.

To add the events simply drag them from the list at the right of the screen to the map as shown in Figures bellow:

© 2002 - 2011 by Optiview USA all rights





The icon of events and their respective sizes can be changed as well as those of cameras. Simply select the desired object and go to Layer options as figure bellow:

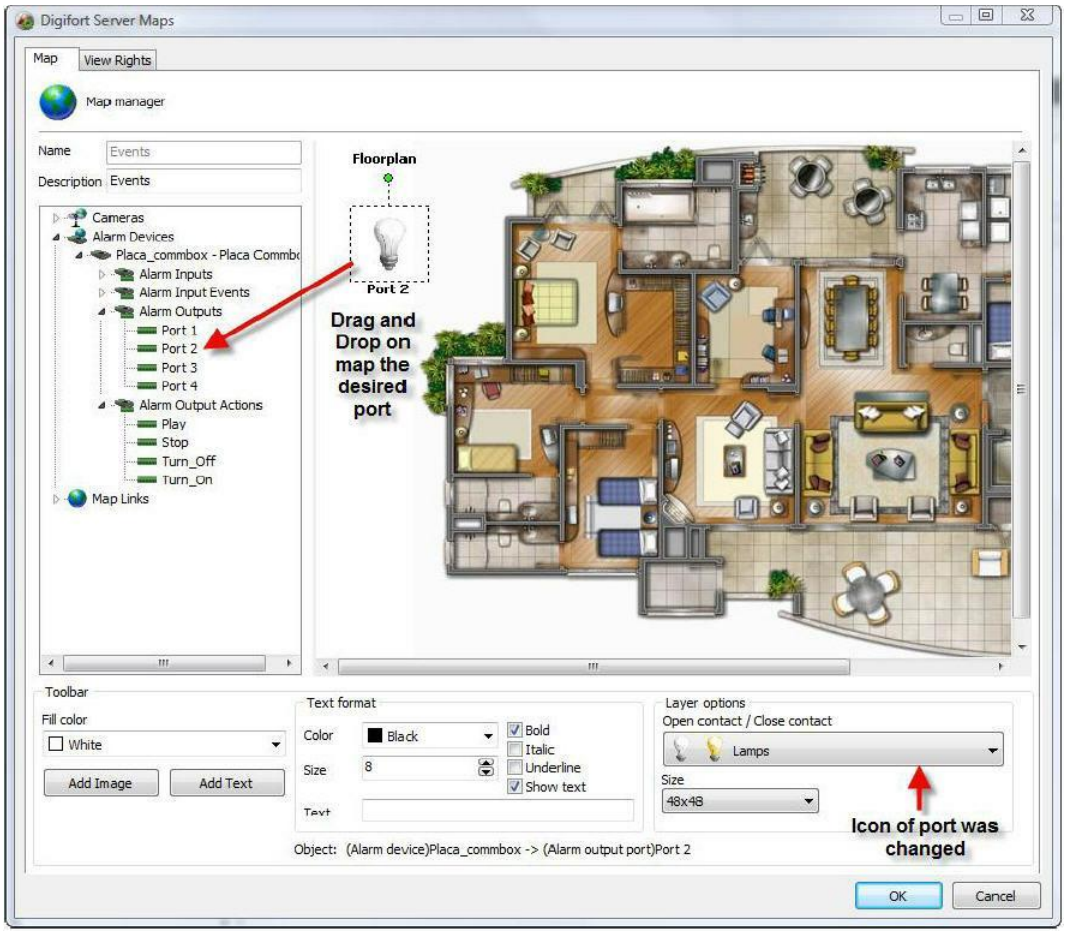
© 2002 - 2011 by Optiview USA all rights



In the case of the figure 8.10, every time someone passes thought the outer fence, Digifort will be alerted and will inform the operator according to the pre-Programmed events. To learn about preProgrammed events, consult How to configure the I/O..

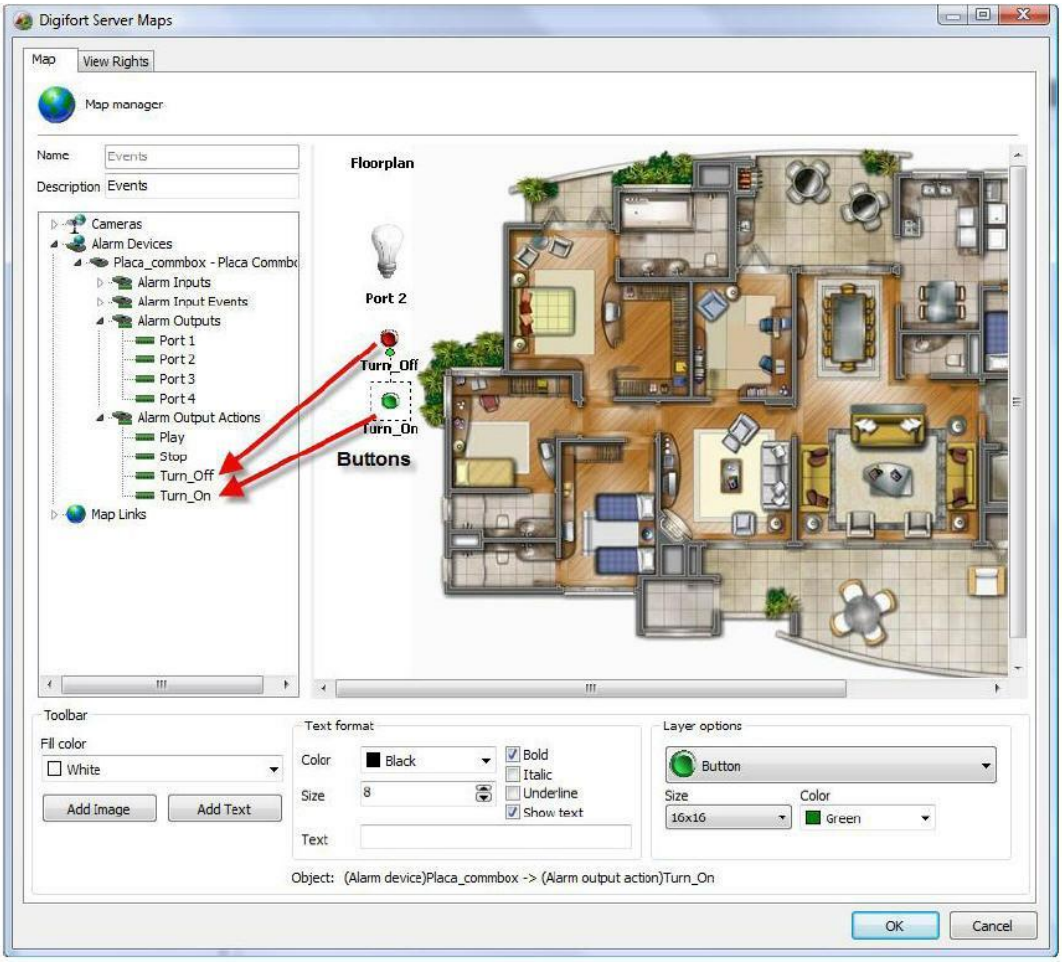
Let's now add an event with buttons. The buttons have the purpose of activating or disactivating an alarm board output via Digifort. To learn how to make events with buttons, consult How to configure the alarm actions

First, drag the port to the map on which the device will be activated is found as shown in Figure bellow:



© 2002 - 2011 by Optiview USA all rights

Now drag the Pre-Programmed buttons to the chosen port as shown in Figure bellow:

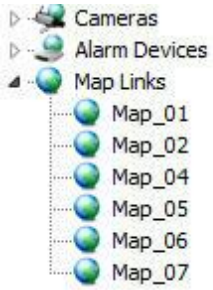


Done! When the map is opened in the Surveillance Client, the alarms will be ready to be activated by the map. To learn how to use the maps in the Surveillance Client, consult its manual.

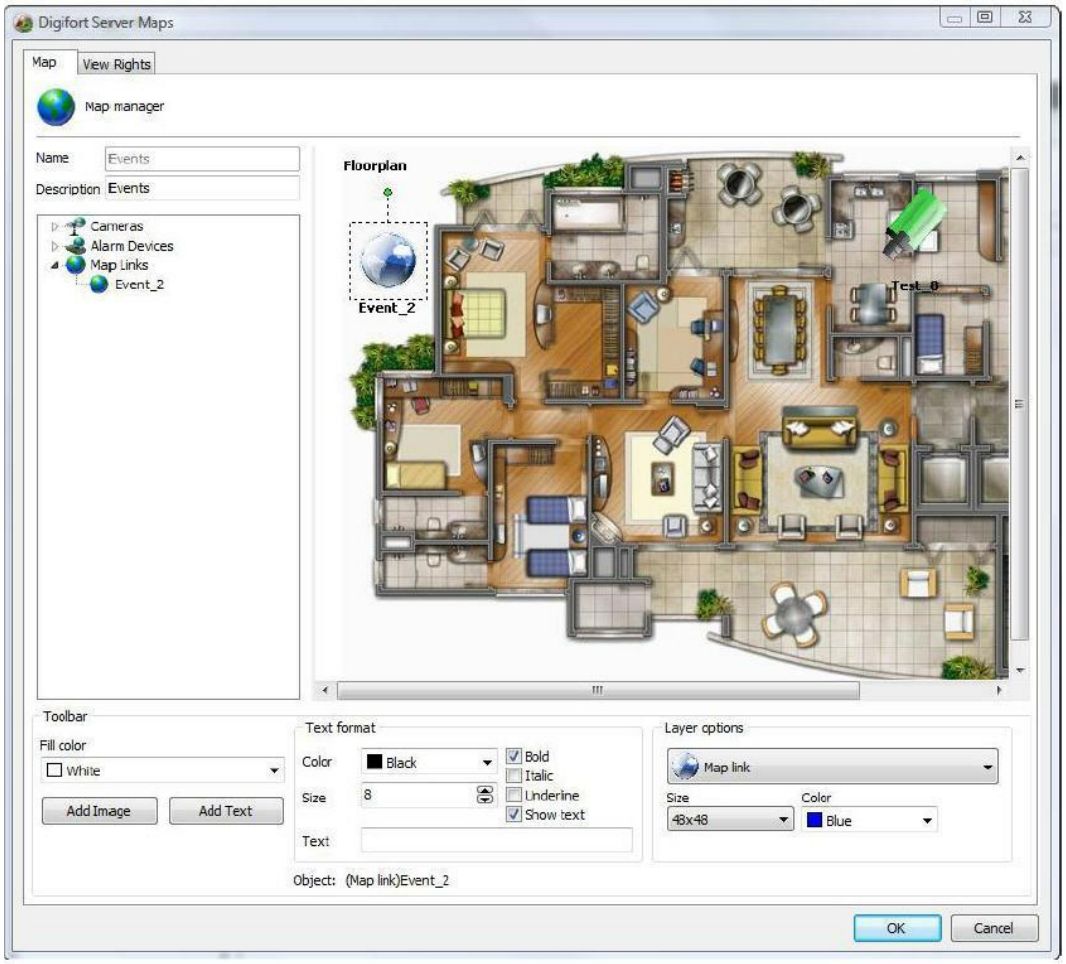
11.1.3 Map Links

The map link is a feature designed to improve administration of maps. Inside a created map you will be able to create links to other maps easing the navigation among them.
To create links it's necessary to have two or more maps registered. When there is more than one map registered besides the one in use, they will appear in the list of maps as shown by Figure bellow:

© 2002 - 2011 by Optiview USA all rights



Click and drag the object to the map as shown by Figure bellow:



Done! Upon opening the map in the Surveillance Client, the icon which is on the screen will call the next map.
Don't forget to put a link on the map to be called to return to the main map, as shown in Figure bellow:

© 2002 - 2011 by Optiview USA all rights



© 2002 - 2011 by Optiview USA all rights

Chapter XII

12 Global Events

Global events are powerful alarm and system integration tools. Like any other event, global events can be used to set off preprogrammed system actions, as well as activate and deactivate the recording of cameras.

Global events can be activated by users by way of the Surveillance Client or by external system, thus allowing any other application to activate an event in Digifort.

This chapter will cover only the configuration of global events. For information on how to activate a global event by way of an external applicatio, consult the API of global events.

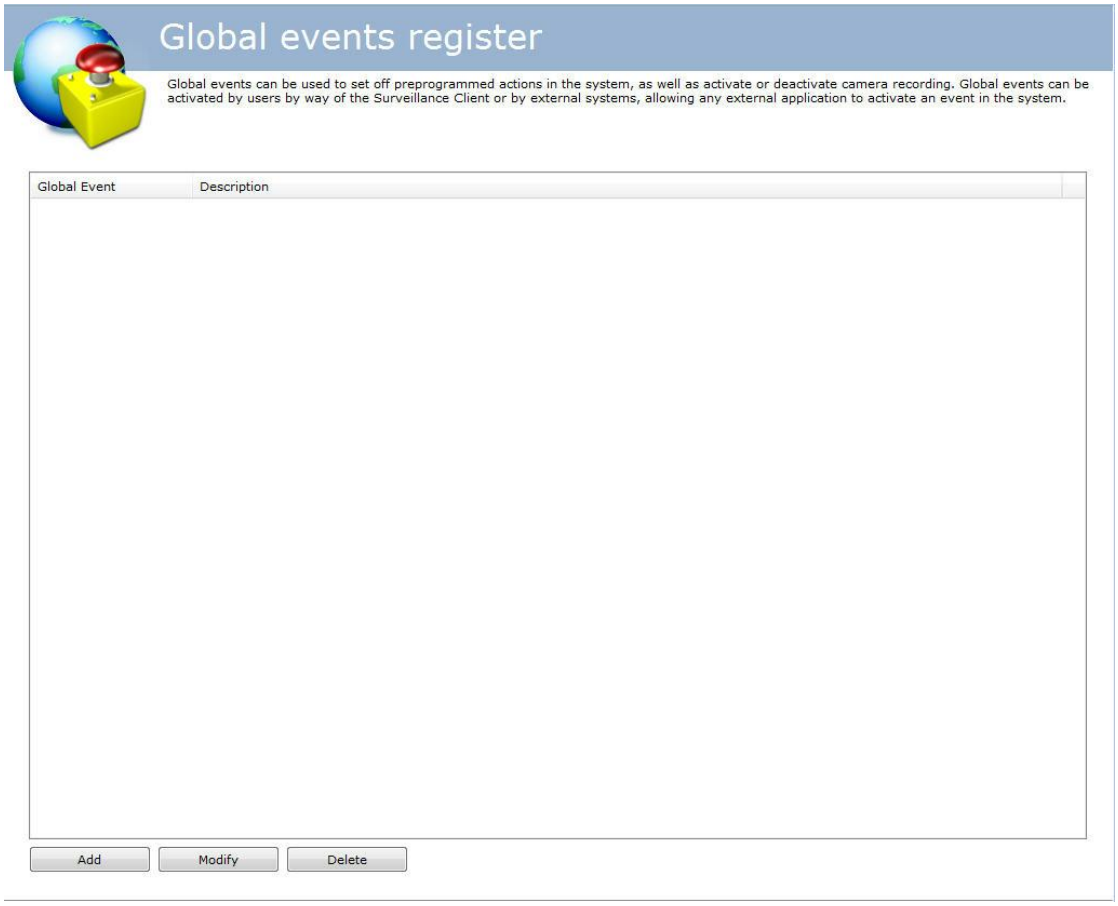
12.1 How to access the Global Events Register

To access the Global Events Register, click on the item Global Events, as shown in the figure bellow.



Once this is done, the alarm devices register will be displayed at the right, as shown in the figure below.

© 2002 - 2011 by Optiview USA all rights


Global events register
Global events can be used to set off preprogrammed actions in the system, as well as activate or deactivate camera recording. Global events can be activated by users by way of the Surveillance Client or by external systems, allowing any external application to activate an event in the system.
Global Event
Description
Add
Modify
Delete

To add a global event, click on **Add**. To modify or exclude, select the desired global event and click on the correspondig button.

12.2 How to add a global event

Once the Add button is clicked, as explained in the topic above, the screen for adding global events will be displayed, as shown in the figure below.

© 2002 - 2011 by Optiview USA all rights



12.2.1 Main data

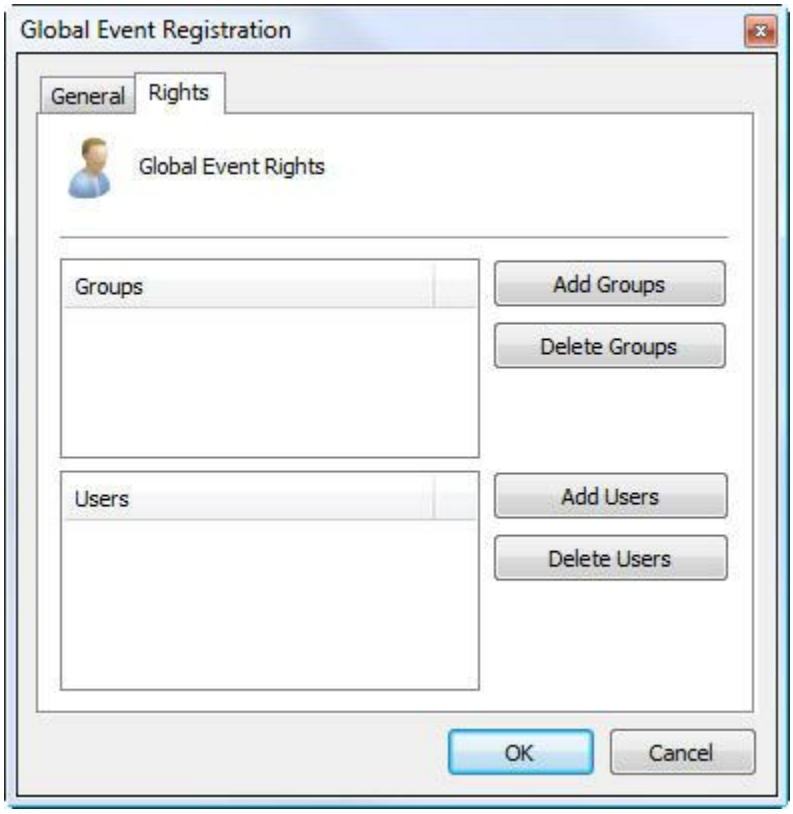
- **Name**: Identification name of the global event. The name of the global event will be used to set off the event in Digifort. After inclusion of the event in the system, the name cannot be modified, as it will be for internal use of the system.
- **Description**: Short description of the global event.
- **Activate**: Enables or disables the global event for use.

To configure the actions of the global event, click on the Configure Actions button. The operational mode of the configuration of the actions is described in Chapter How to configure the alarm actions

12.2.2 Rights

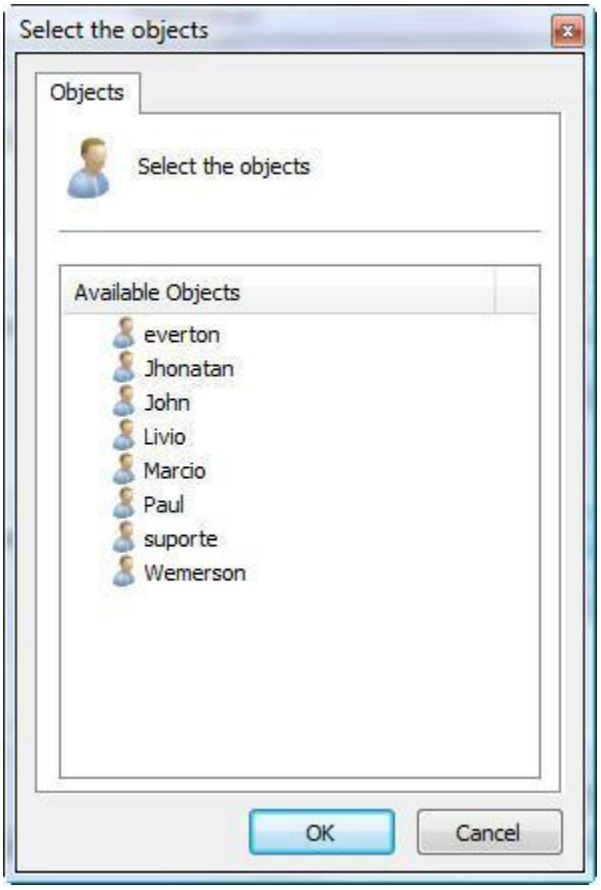
Global events can have access restricted to some users of the system. To attribute user rights, click on the **Rights** tab, as shown in the figure below:

© 2002 - 2011 by Optiview USA all rights



To conceed the right of access to the desired users/groups, simply click on the **Add Grupos/Users** button and select them in the list of **Groups/Users** which will appear as the figure shows.

© 2002 - 2011 by Optiview USA all rights



Select the available User and click on **OK**. The same rule applies to the list of groups.

© 2002 - 2011 by Optiview USA all rights

Chapter XIII

13 Analytics

The analytics is a set of tools that intelligently processes the cameras' images. This process includes object count, flow control, missing and foreign objects, face detection and others shown in more detail below.

The analytics can complement surveillance in several ways, such as by triggering alerts, filing events and generating reports.

The Digifort analytics is considered an extra module as it is not included in the license of the Digifort cameras' server.

The Digifort Analytics has a server/own service for processing images and which can be installed on the same computer in which the camera images are recorded or in another computer used only for this purpose (recommended). Learn more about distributed processing in the chapter Understanding distributed processing.

13.1 Licensing the Digifort Analytics

How does the architecture for the Digifort Analytics work?

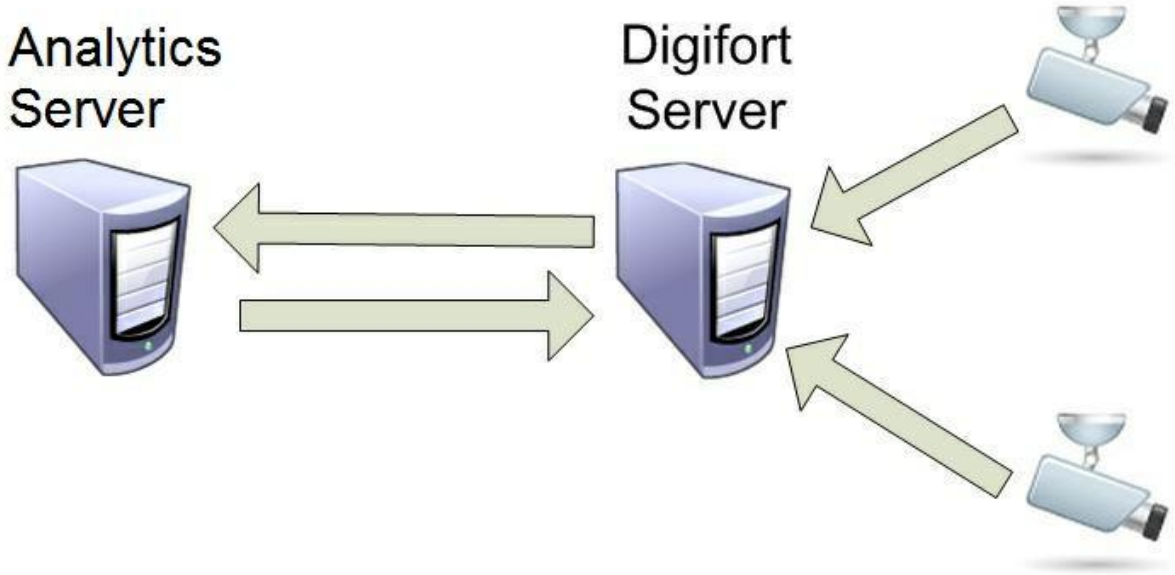
The license for the Analytics server works like the server for the Digifort cameras. There is a "base license" for the server and "additional licenses" for each camera.

The Digifort Analytics' base license includes the "Basic Analytics" which has the following modules: **Foreign Objects, Missing Objects and Face Detection** which can be used in as many cameras as needed.

The licenses for cameras (better known as "license pack") include de license for the **Advanced Analytics** which has the following modules available: **Presence, Entry, Exit, Disappear, Motionless, Loitering, Direction Filter, Speed Filter, Camera Tampering, and Cancel Shaking.**

The following diagram shows the licensing of two cameras with video analysis (**Basic** and **Advanced**) together with the Digifort server:

© 2002 - 2011 by Optiview USA all rights



In the picture above, the license distribution would be as follows:

- Analytics Server**: 1 licença base de analítico + 1 licença pack para 2 câmeras.**
- Digifort Server**:** 1 Base license (the version's base license Enterprise already includes 8 licenses available for recording; if the number of cameras added surpasses the number of base licenses, license packs should be added).

13.1.1 Understanding the distributed processing

In terms of processing, video analysis is heavier than recording/viewing from a camera. With flexibility in mind, Digifort developed an innovative processing architecture – the distributed processing architecture.

Digifort allows the cameras' analytical processing recorded on the Digifort server to be carried out on one or more computers that include the Analytical Server. The major advantage is that with such flexibility the recording server does not become overloaded and does not need to be a "super machine".

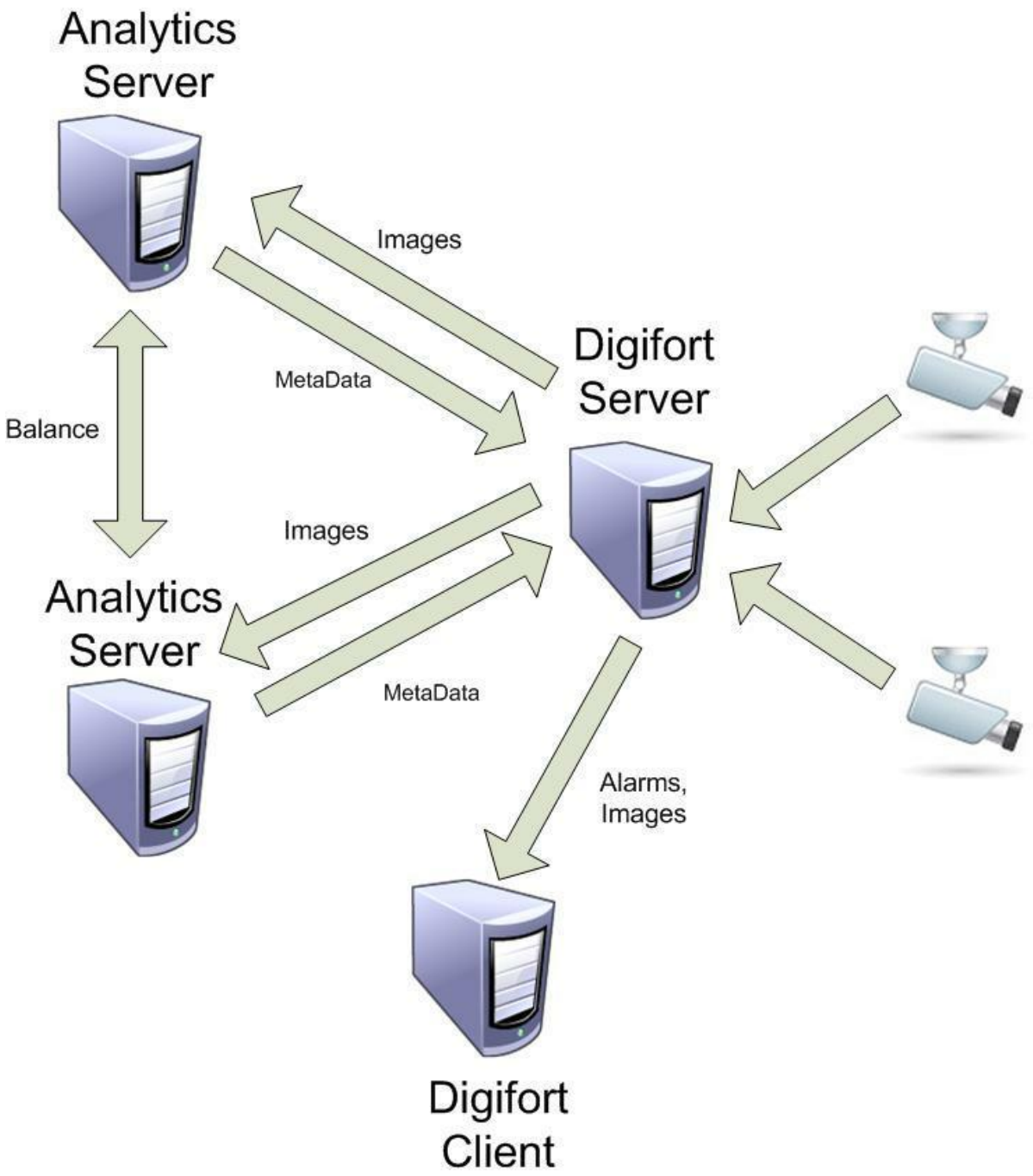
The analytical server automatically checks the computers with smaller processing capacity and "counterbalances the load", in other words, it distributes the processing of the video analyses so

© 2002 - 2011 by Optiview USA all rights

that all computers are left with as little processing as possible.

Remember that each computer with distributed processing is licensed with the Digifort Analytics base license.

Look at the diagram below:



© 2002 - 2011 by Optiview USA all rights

In the diagram above, the "**Digifort Server**" records the cameras' images and sends them to the " **Analytics Servers**" which, in turn, carry out their analyses and return the metadata (information on the alerts generated, object positioning and alert areas). The load counterbalance is among the "Analytics Servers" if it has been configured to do so. When the metadata return to the Digifort Server, it sends them and the alerts to the "**Digifort Clients**" (Surveillance Clients).

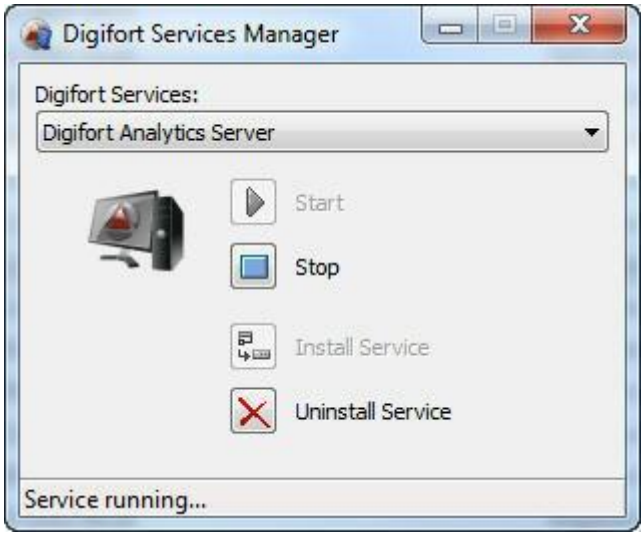
13.1.2 How to start the Analytics Server

To start the Digifort Analytics Server it must first be installed. Follow these steps to start the service correctly:

1. Select the "Digifort Analytics Server" service.

2. Click on Install Service. A confirmation screen will open indicating the service has been successfully installed.

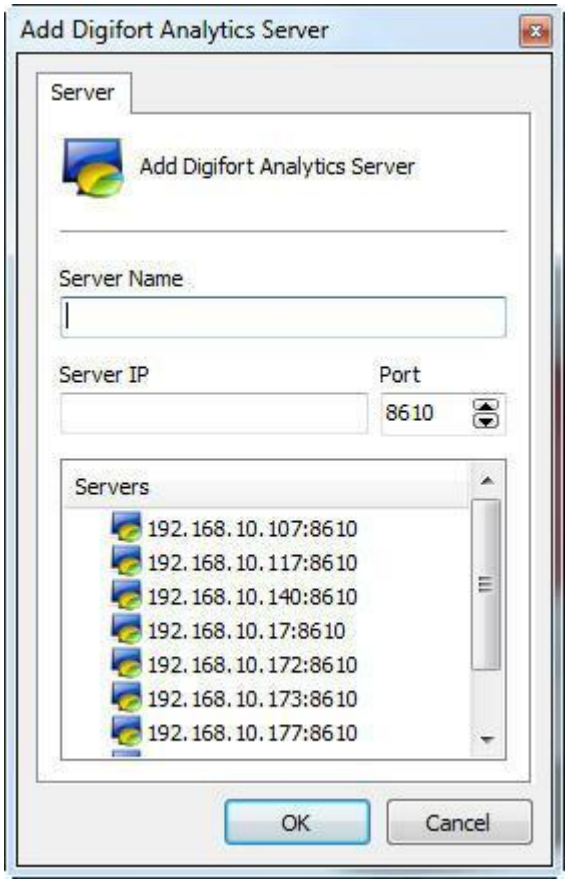
3. Click on Start and wait while the server initializes. The start process ends when the message "Service in operation..." shows on the status bar.



13.1.3 How to configure the servers to be managed

The first step to configure an analytics server is to add it to the list of servers to be managed by the Administration Client.
To add a server, click on the **Digifort Analytics Servers** diagram and then on the **Add Server** button, and the screen with the server registration will open as shown below:

© 2002 - 2011 by Optiview USA all rights

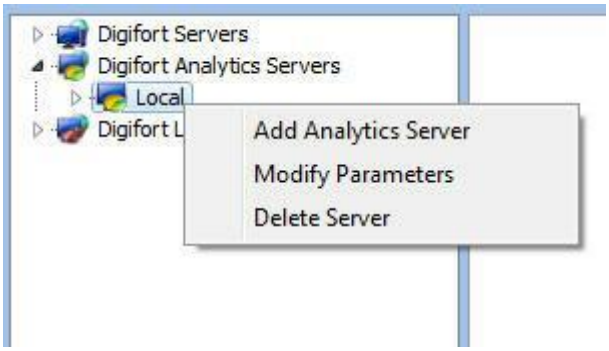


- **Server Name**: Type the name of the server to be added. Once the data has been confirmed, the server name cannot be altered.
- **Server IP**: Type the name of the server to be managed.
- **Port**: Type the communication port with the server. By default, the port is 8610. The communication port with the server cannot be altered. This configuration should only be altered if you are accessing a remotely located server, such as the Internet, for example.
- **Servers**: This list comprises all the Analytics servers found on the network by the administration client. By clicking on one of the servers, the IP and **Port** described above are automatically filled in and all you have to do is fill in the **Server Name** to register.

Once you have provided all the correct data, click on **OK**.

When it has been included in the server, it will come up on the **Configurations** Menu as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights

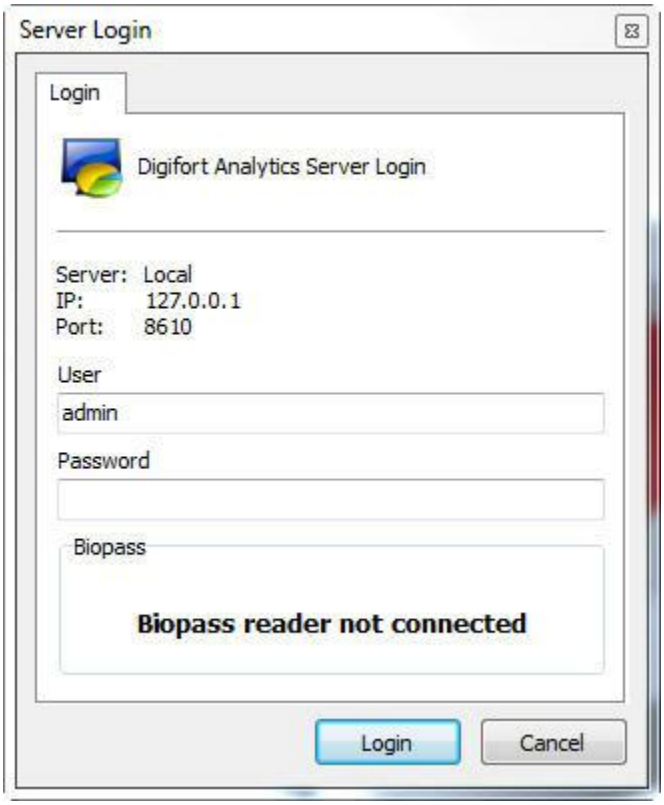


To change the parameters of a server previously saved, click with the right-hand button of the mouse on the server chosen and click on Change Parameters. Change the data as necessary on the window that opens and click on **OK**.

To remove a server, click with the right-hand button of the mouse on the server chosen and then click on **Remove Server**. On the confirmation message that shows up click on **Yes**.

13.1.4 How to connect a management server

After adding the server, locate in it in the Configurations Menu and double-click on it. Once this is done, you will be asked to provide a username and password to access the server configurations as shown in the picture below:



© 2002 - 2011 by Optiview USA all rights

- **Username:** Access username.
- **Password:** Password for access.

Enter your username and password to access the server or the biometrics. If this is the first time you are accessing the system, insert the same username as the admin and leave the password blank.

Once you have filled in the access information, click on **OK**. If the authentication for access is successful, the Configurations Menu opens showing the configurations available for the server, as shown in the picture below:

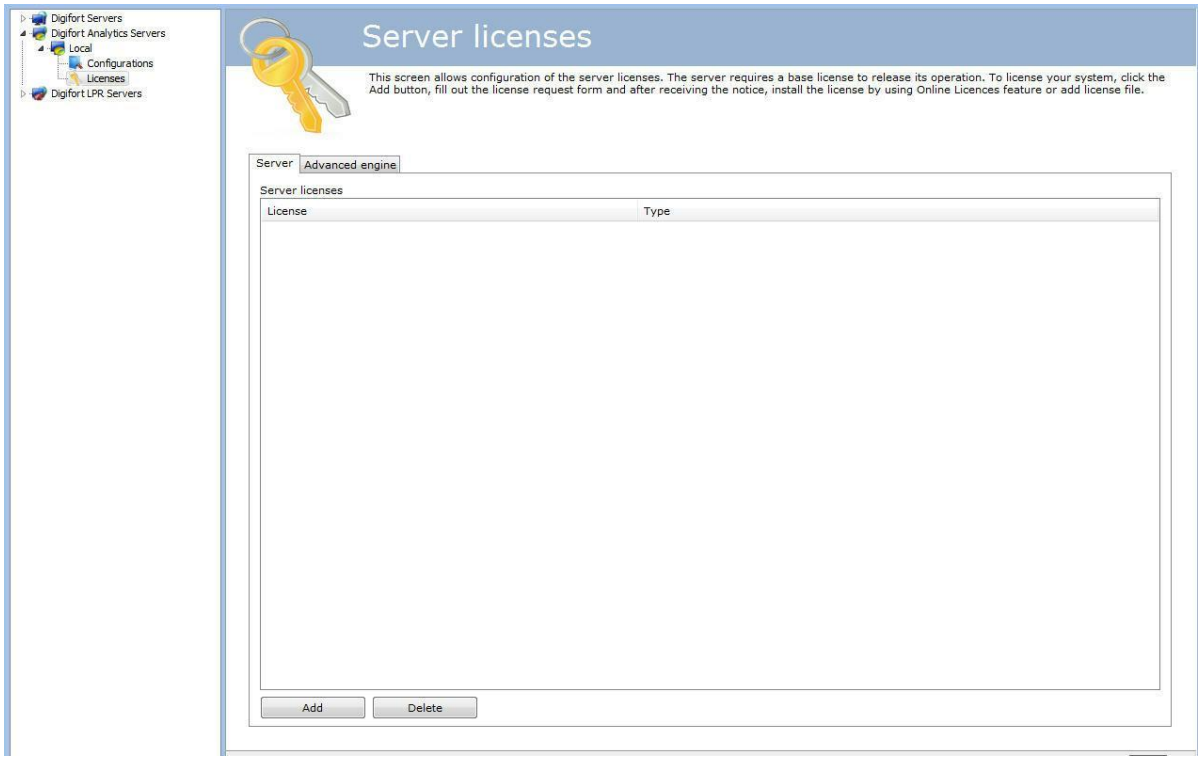


13.1.5 How to configure the analytics licenses

As said before, the Analytics works with two types of licenses: the Base License (**Basic**) and the License Pack (**Advanced**).

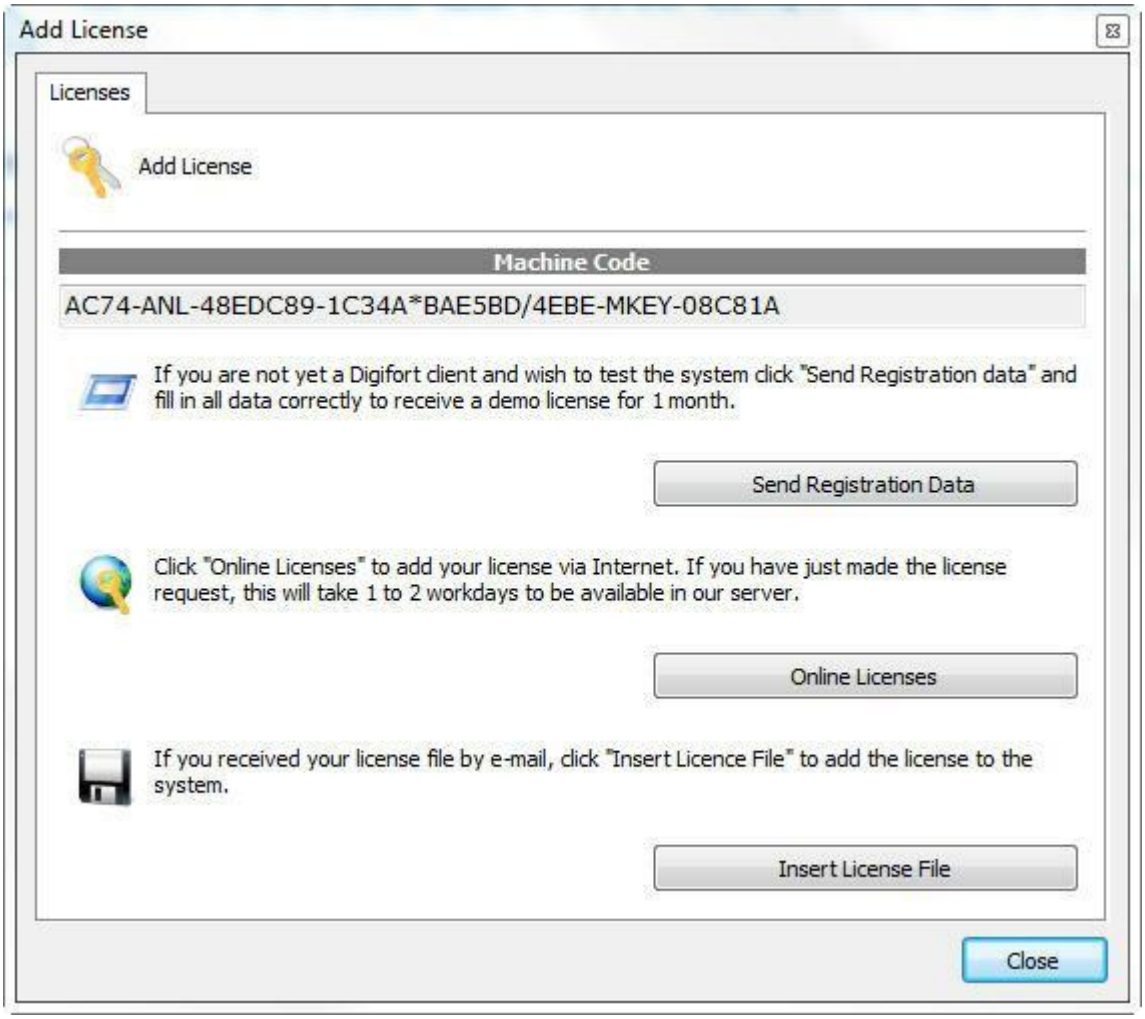
The first step to license the analytics is to add the base license (**Basic**). Once connected, go to the licenses field as shown below:

© 2002 - 2011 by Optiview USA all rights


Digifort Servers
Digifort Analytics Servers
Local
Configurations
Licenses
Digifort LPR Servers
Server licenses
This screen allows configuration of the server licenses. The server requires a base license to release its operation. To license your system, click the Add button, fill out the license request form and after receiving the notice, install the license by using Online Licences feature or add license file.
Server
Advanced engine
Server licenses
License
Type
Add
Delete

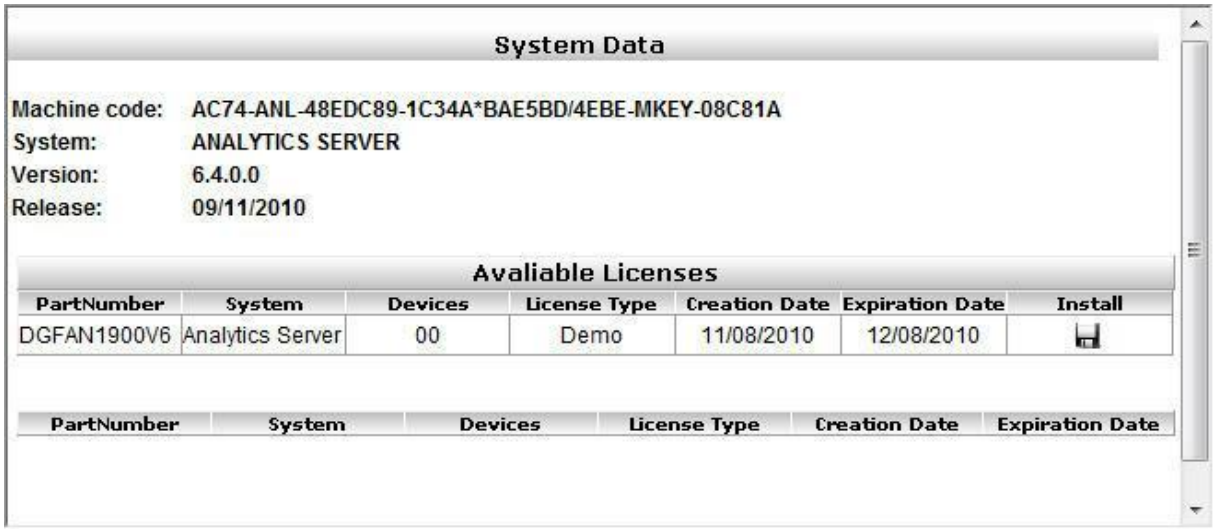
To add a license, click on Add and the following screen will show up:

© 2002 - 2011 by Optiview USA all rights


Add License
Licenses
Add License
Machine Code
AC74-ANL-48EDC89-1C34A*BAE5BD/4EBE-MKEY-08C81A
If you are not yet a Digifort client and wish to test the system click "Send Registration data" and fill in all data correctly to receive a demo license for 1 month.
Send Registration Data
Click "Online Licenses" to add your license via Internet. If you have just made the license request, this will take 1 to 2 workdays to be available in our server.
Online Licenses
If you received your license file by e-mail, click "Insert Licence File" to add the license to the system.
Insert License File
Close

The procedure to add licenses is the same as for Digifort and is described in the chapter How to configure licenses .
On the online license screen the description should be "**Analytics Server**" as shown in the picture below:

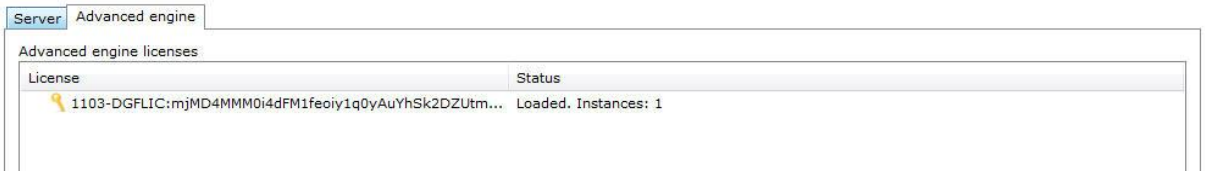
© 2002 - 2011 by Optiview USA all rights


System Data
Machine code: AC74-ANL-48EDC89-1C34A*BAE5BD/4EBE-MKEY-08C81A
System: ANALYTICS SERVER
Version: 6.4.0.0
Release: 09/11/2010
Avaliable Licenses
PartNumber System Devices License Type Creation Date Expiration Date Install
DGFAN1900V6 Analytics Server 00 Demo 11/08/2010 12/08/2010
PartNumber System Devices License Type Creation Date Expiration Date

Once a license has been added it becomes available as shown in the picture below:



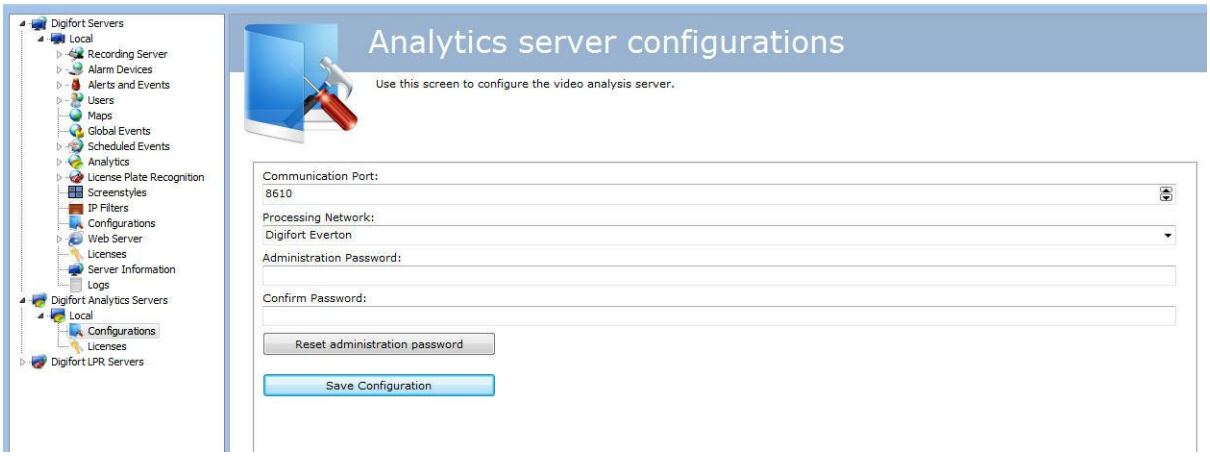
The **Advanced** analytics license works in the same way and in the status field you can see how many licenses are available, as shown in the picture below:



13.2 Analytics Server Configurations

To access the analytics server configurations, click on **Configurations** as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights

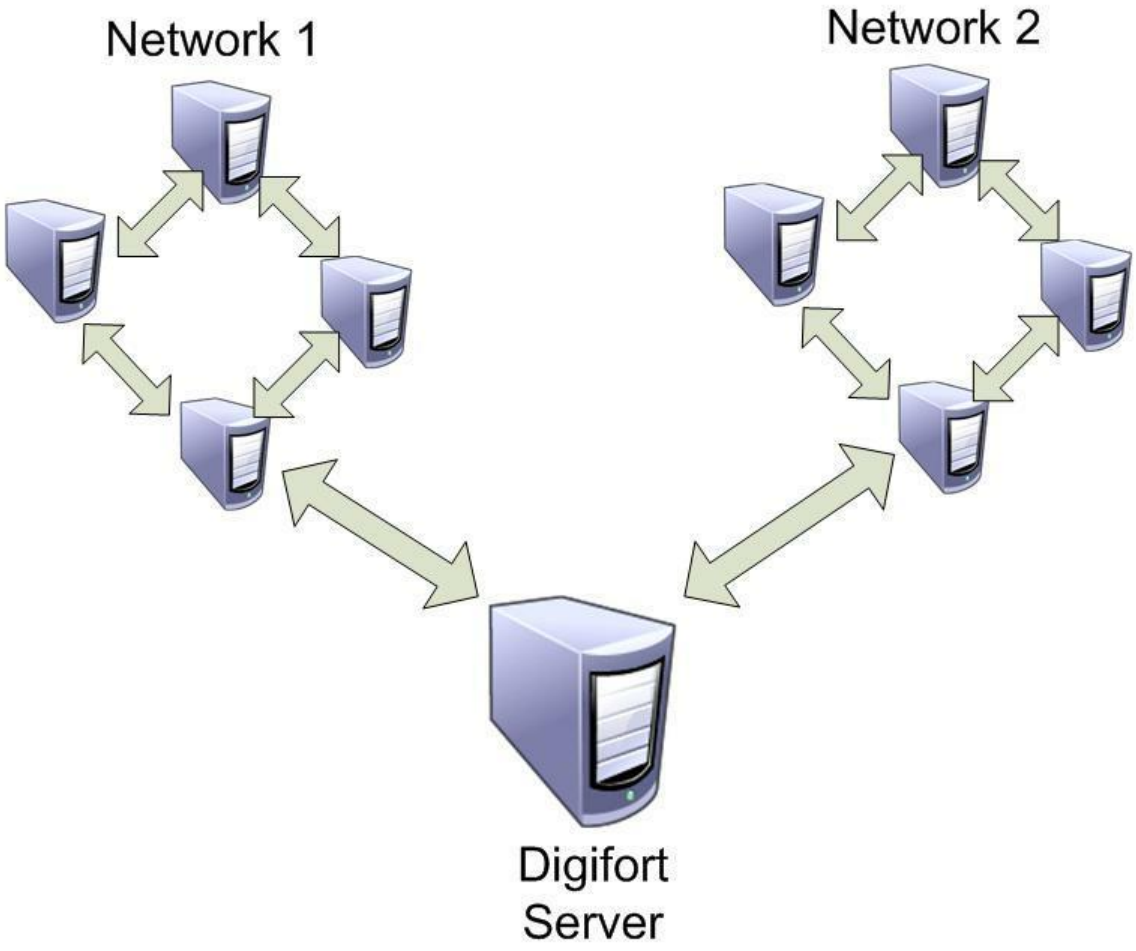


This screen has the following functionalities:

Communication Port: Communication port with the analytics server. It should only be changed if it is already being used on the computer in question.

Processing Network: Name of the distributed network where the server will counter balance the load. When more than one server has the same "Processing Network" name there will be a processing counterbalance among them. Look at the diagram below to get a better idea:

© 2002 - 2011 by Optiview USA all rights



In the picture above, the "**Digifort Server**" sends the images of the cameras to two different " **Processing networks**". This way, each set of computers only counterbalances the load among the **Analytics Servers** with the same network name.

Administration Password: Password to access the analytics server. Fill in this field to change the current password.

Confirm Password: Type the password again.

Reset administration password: Blank password is retrieved.

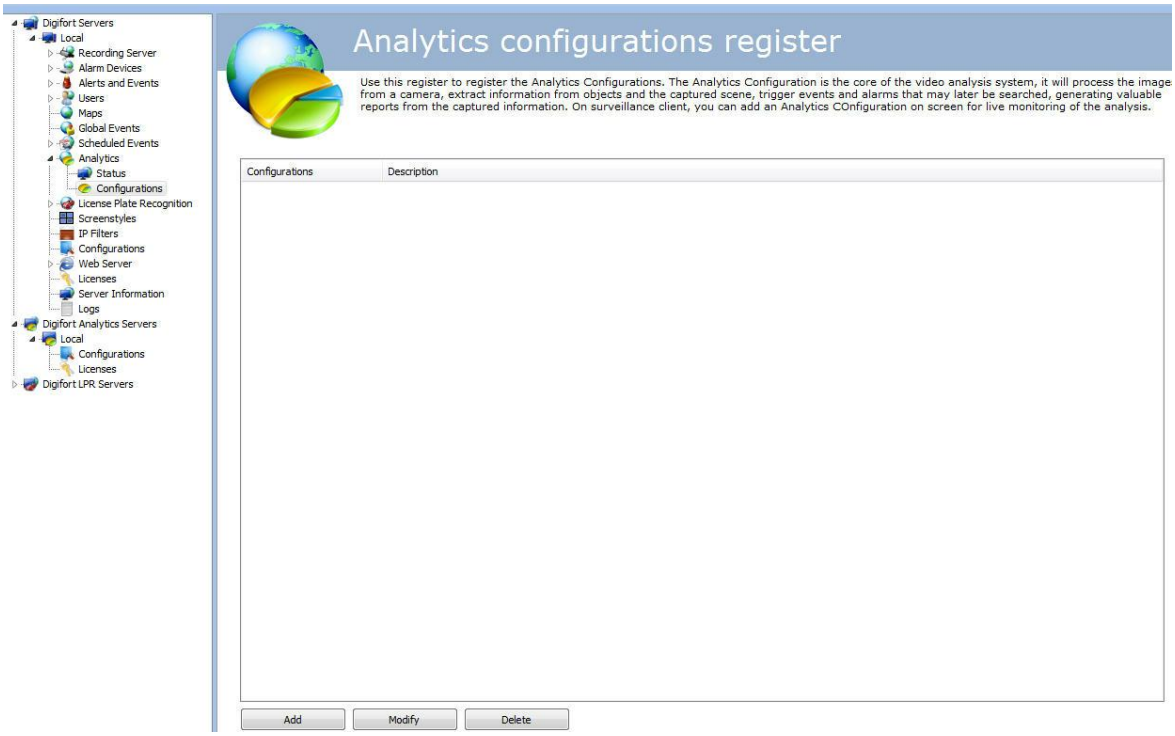
Save configurations: Saves changes made on the screen.

13.3 Adding an analytics configuration

This topic will deal with how Digifort's **Basic** and **Advanced** analytics are configured.

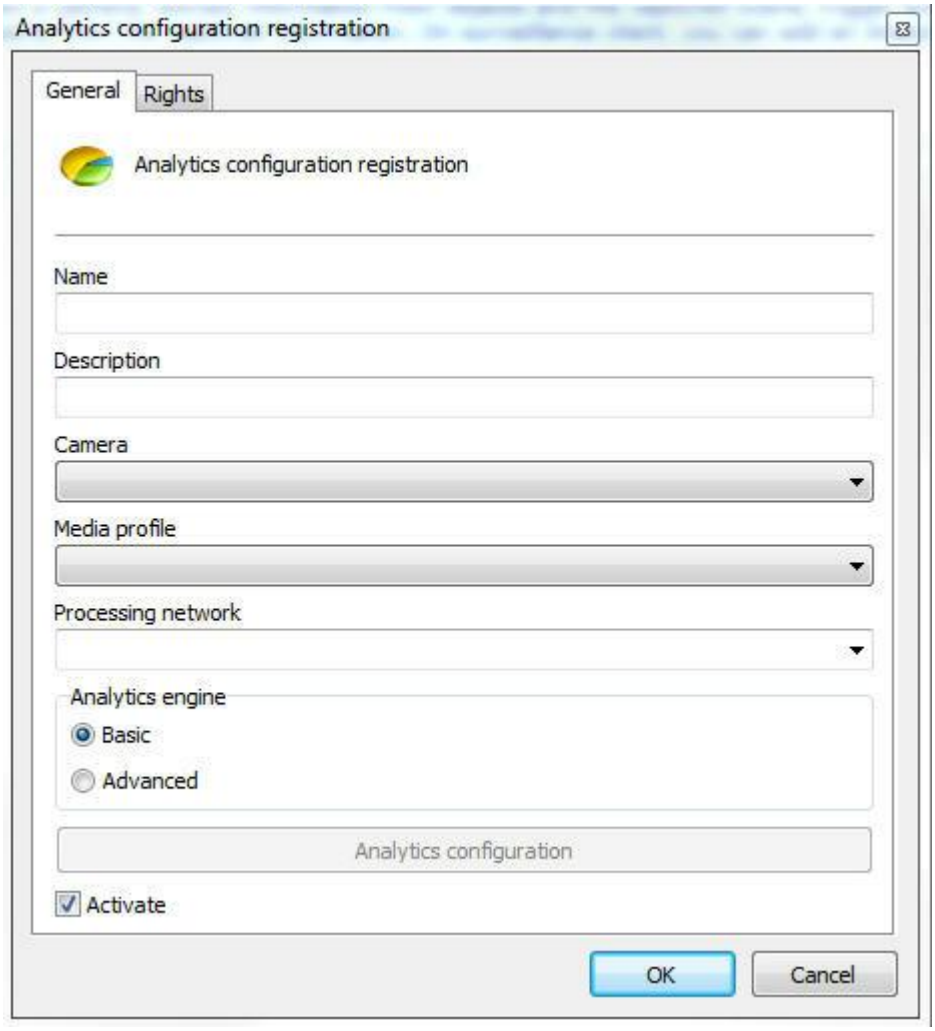
After licensing the analytics server correctly, go to the analytics **Configurations** as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



In this screen, click on the **Add** button to start the analytics configuration. The following screen will show up:

© 2002 - 2011 by Optiview USA all rights



This screen has the following functionalities:

Name: Name of the analytics chosen, for example: **Digifort**.

Description: Description of the analytics register, for example: Vehicle count on avenue.

Camera: All the cameras registered in the Digifort server will be available in this selection box. To learn how to register cameras, refer to the chapter How to add a camera .

Media profile: Select the media profile you want to use for the analysis. The analytics always analyses images with a resolution of 320x240 or 352x240, so it is recommended that these are the camera's minimum values. The video analysis does not interfere with the quality/performance of the video transmitted and recorded.

Processing Network: All the "processing networks" (analytics servers) active on the network will be available in this field. Choose a network to process that configuration.

Analytics Engine: Choose the engine that will be analyzing the images. Digifort has two engines that process the images: the Basic Analytics and the Advanced Analytics.

© 2002 - 2011 by Optiview USA all rights

The **Basic Analytics** has the following analysis modules: Foreign Objects, Missing Objects and Face Detection.
The Advanced Analytics has the following analysis modules: **Presence, Entry, Exit, Disappear, Motionless, Loitering, Direction Filter, Speed Filter, Camera Tampering, and Cancel Shaking.**

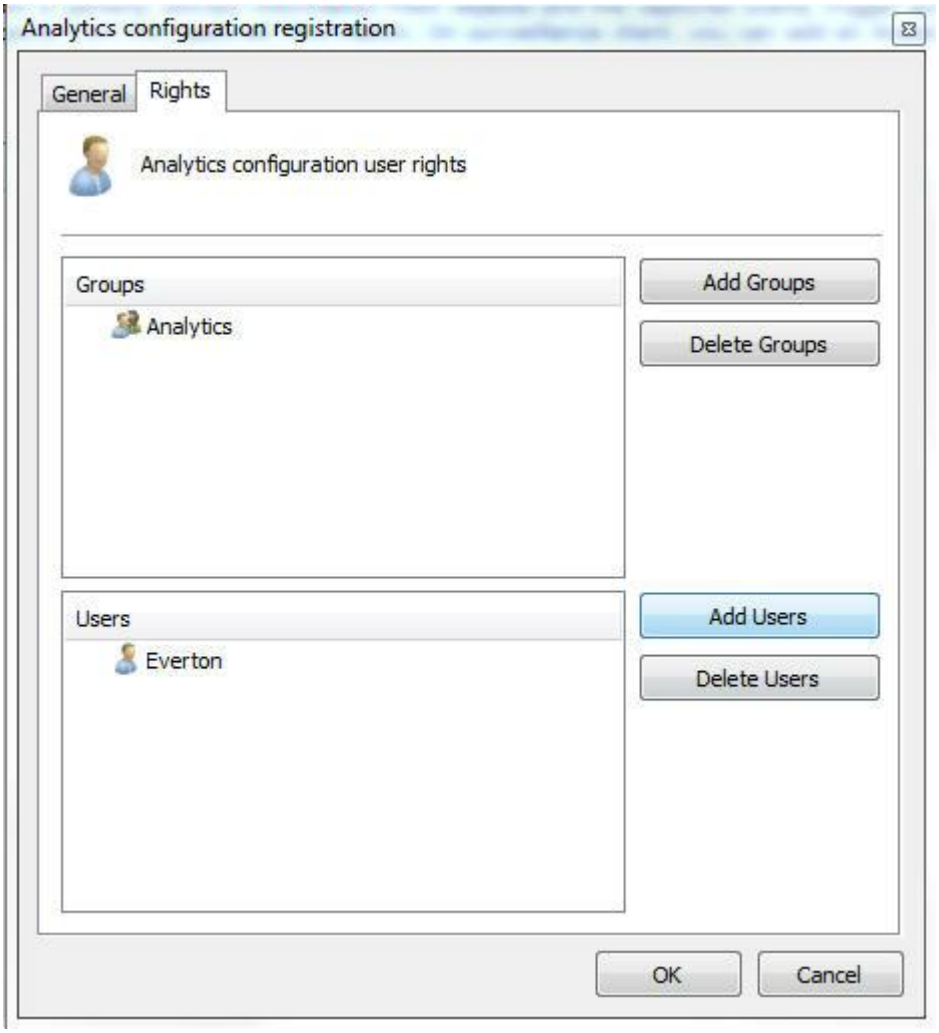
Analytics configuration: Opens the configuration screen of the chosen engine.

Activate: Activates or deactivates the analytics configuration.

Note

A license is used when an Advanced analytics configuration is active

In the configurations screen it is still possible to configure which users will be able to see this configuration. See the picture below:

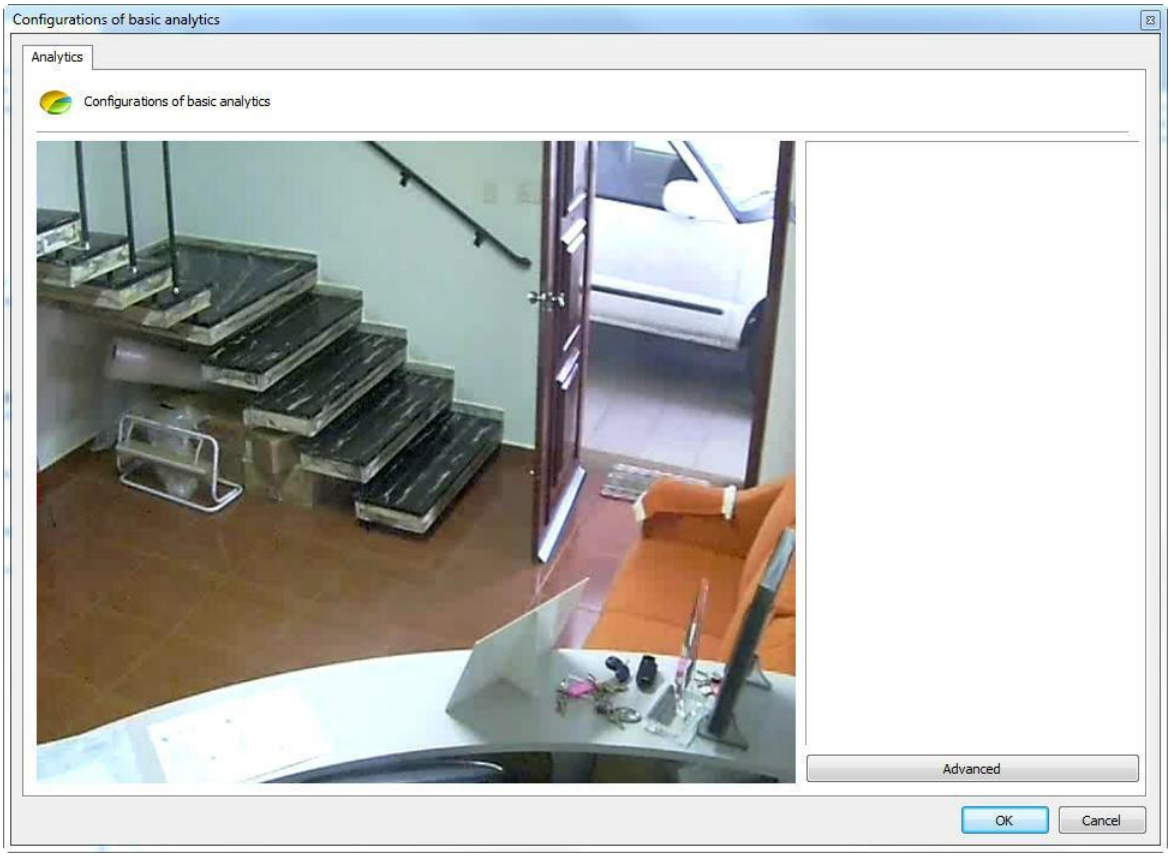


To learn about users and user groups refer to the chapter User Management .

© 2002 - 2011 by Optiview USA all rights

13.3.1 How to configure the Basic Analytics

If the **Basic** engine is chosen in the analytics register screen, the following screen will show up:



The image that appears is related to the camera and the media profile selected in the register screen of the analytics.

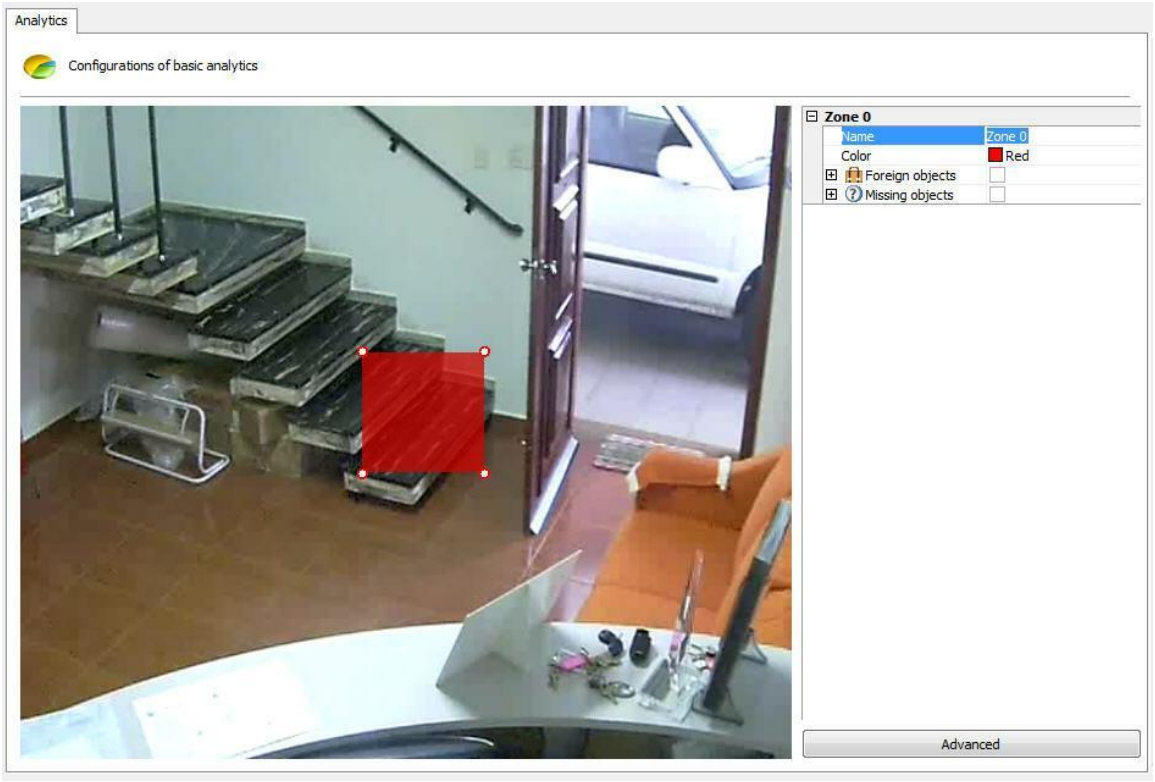
This screen has the following functionalities when the right-hand button is activated:



- **Create zone**: Creates a zone where the analysis module is defined.
- **Delete**: Deletes a selected zone.

Create a zone and click on it as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights

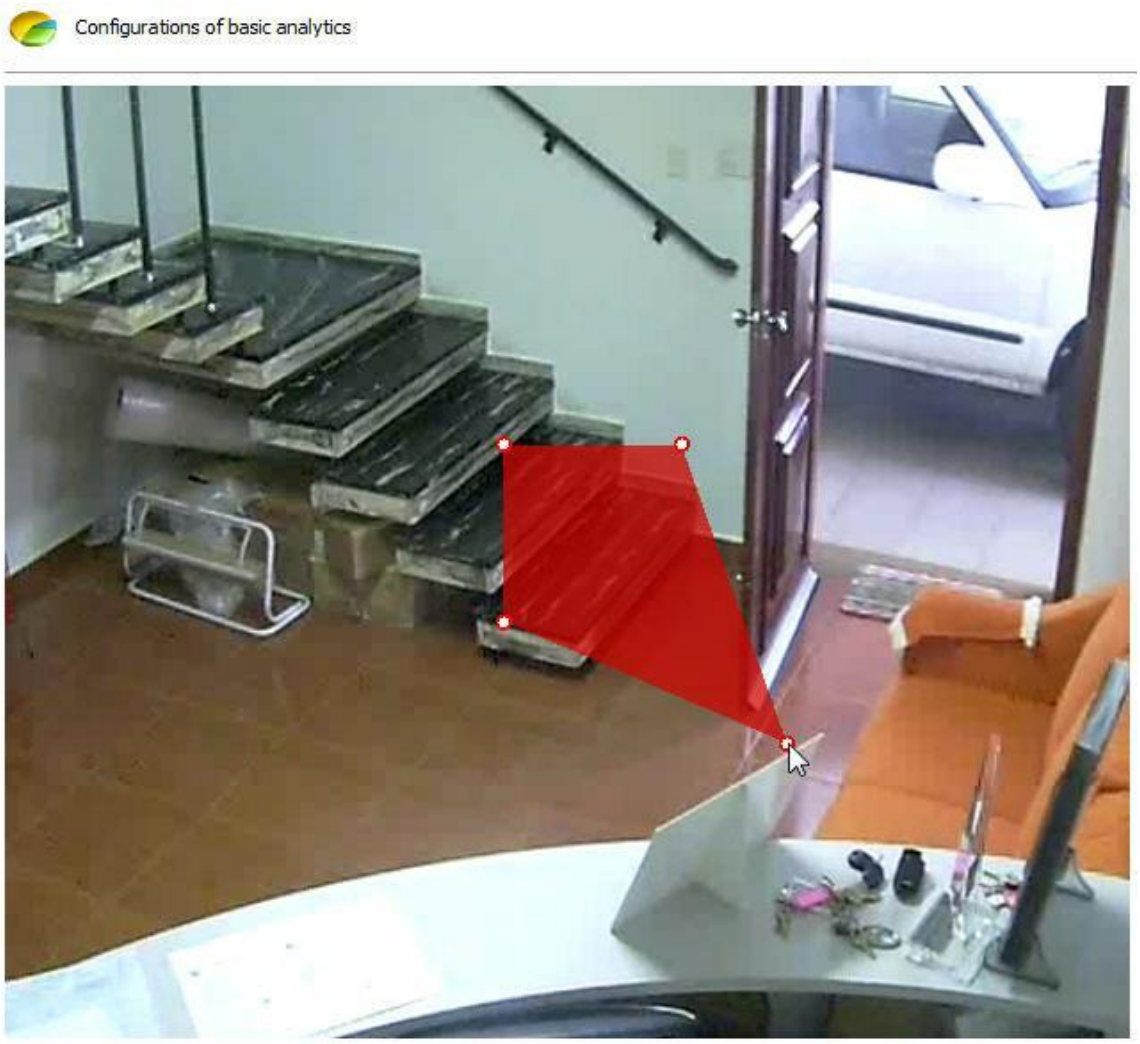


An options menu of the area will open on the screen's right-hand column. The following options will be available:

- **Name**: Name for the area created. It is important to consider what name will be given as it will be possible to create reports using that name.
- **Colour**: Changes the colour of the area selected.
- **Foreign Objects**: Module that analyzes the objects left. This module will be described in chapter Foreign Objects
- **Missing Objects:** Module that analyzes the objects removed. This module will be described in chapter Missing Objects

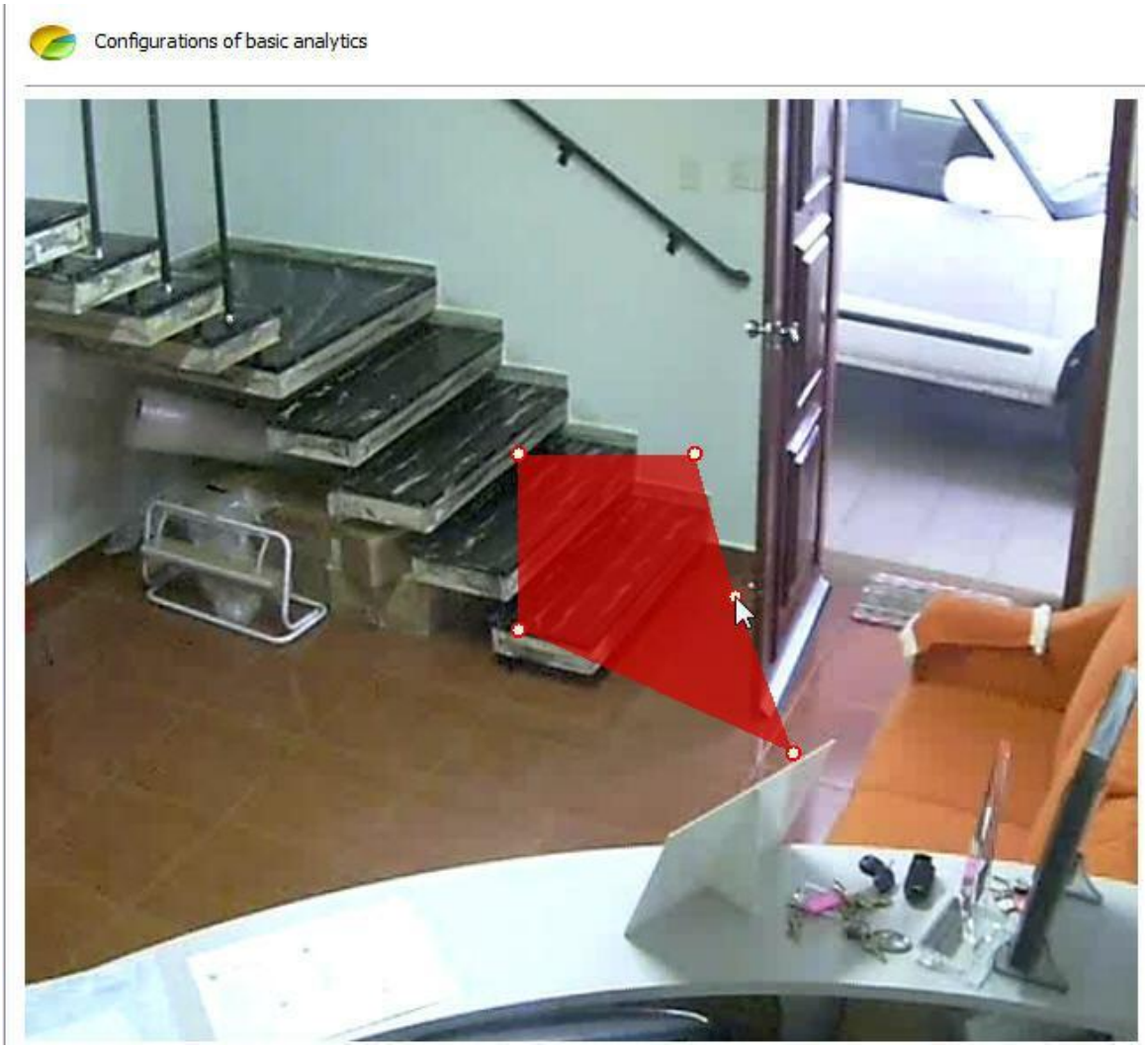
You can move the points in the area by clicking on the circles, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



And add points with a double-click near the area's edge as shown below:

© 2002 - 2011 by Optiview USA all rights



20 is the maximum number of points per area.

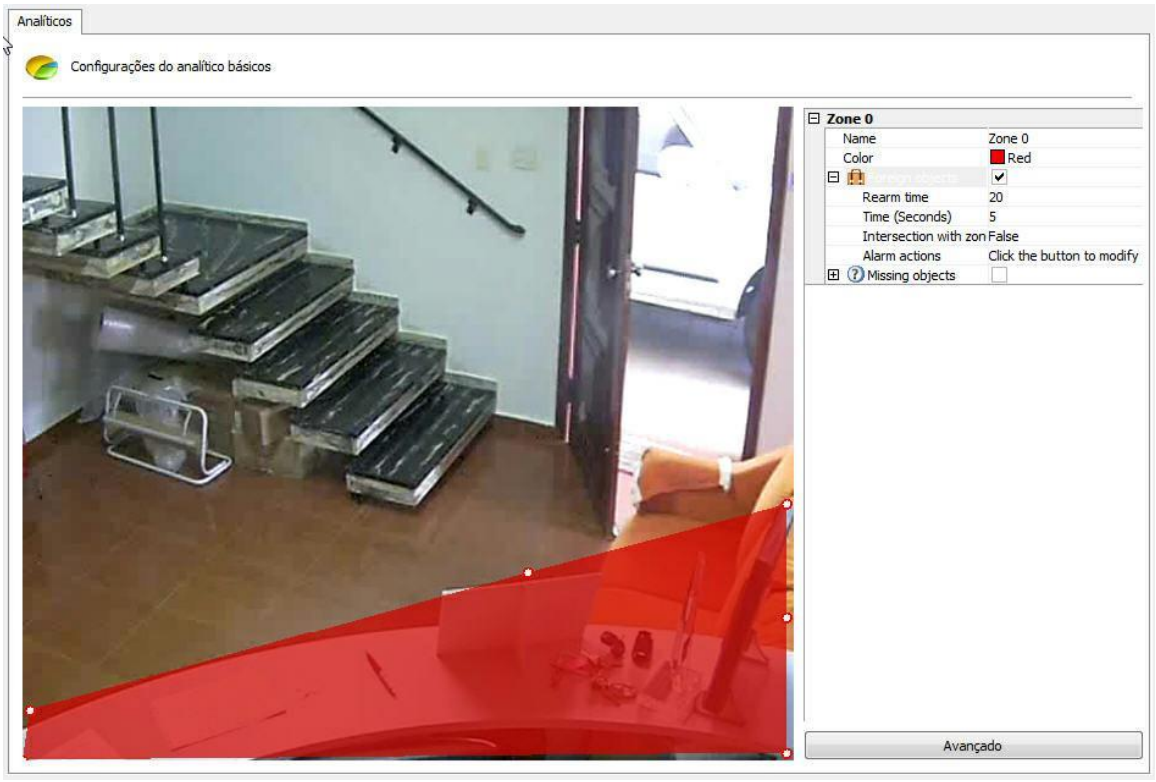
13.3.1.1 How to configure the Foreign Objects module

The **Foreign Objects** module can generate alerts when an object is left in a specific area of the image or when something in the scene changes. Example: A bag left on the floor; a key found on a table. The video can be recovered from these events, and alerts and reports generated.

The analytics modules were designed to help surveillance and are not 100% precise. For example: the foreign objects module can create alerts if there are changes to the lighting, projected shadows, etc. and this creates the so-called false alarm.

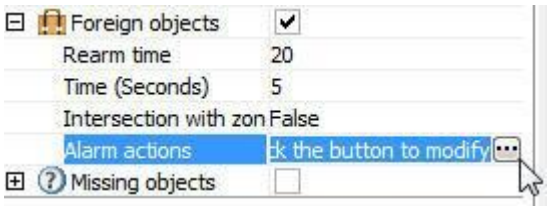
In our example, we created a detection area for the table as in the picture below:

© 2002 - 2011 by Optiview USA all rights



By opening the side options in **Foreign Objects**, the following functionalities are available:

- **Foreign Objects:** Tick this option to activate the Foreign Objects in this area.
- **Rearm time**: Rearm time for the alert to be activated again in the surveillance client (if configured).
- **Intersection with the area**: If false it will only be triggered if there are objects with their centre within the zone. If true, any object intersecting with the area can trigger the alert.
- **Time**: Time in seconds the object must remain unmoving in the area to trigger the alert. Long periods are not recommended for areas where there is a lot of movement.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alert actions.

The following is an example of when the alert was triggered in the situation previously configured:

© 2002 - 2011 by Optiview USA all rights



Whenever an alert is triggered the scene is automatically captured.
To learn how to generate reports, refer to the Surveillance Client manual.

Nota

The Foreign Objects module will trigger alerts if there is any change in the scene, in other words, whenever objects are left or removed. The difference between this module and the Missing Objects one is that this one looks for objects within an area, whereas the Foreign Objects module outlines the area exactly around the object in question.

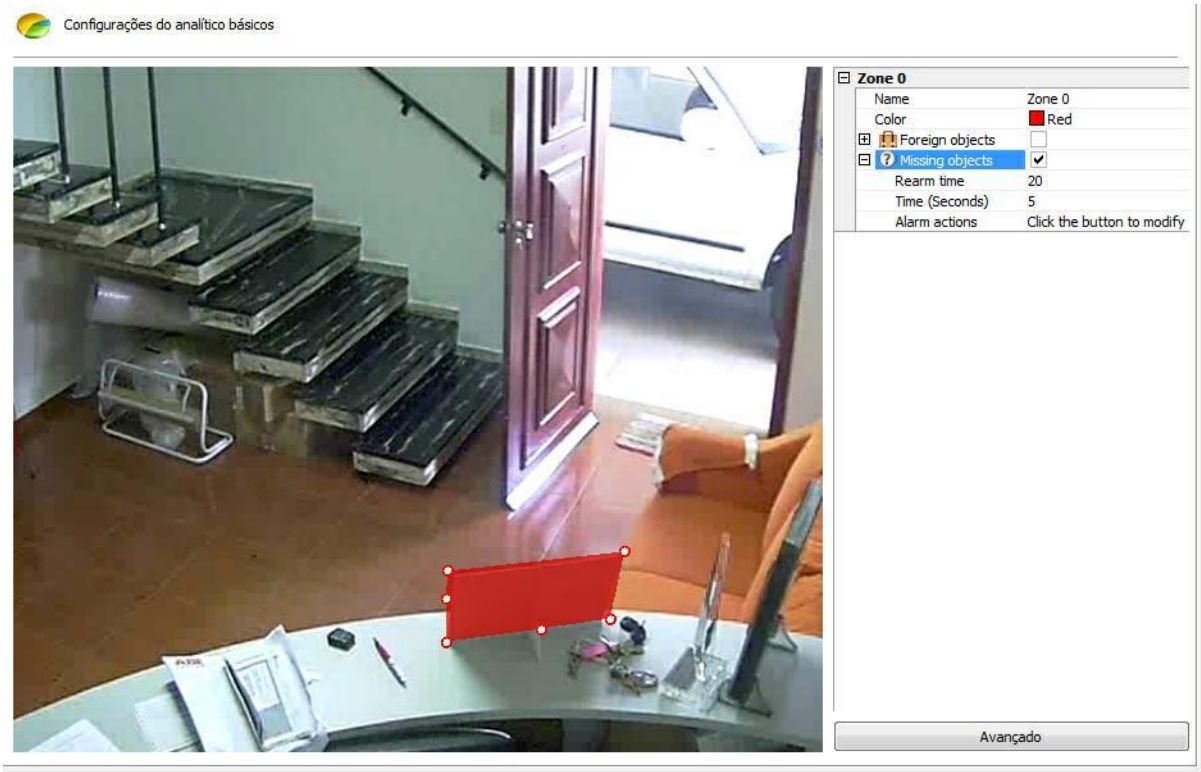
13.3.1.2 How to configure the Missing Objects module

The **Missing Objects** module can generate alerts when a delimited object is removed from the scene. Example: A picture, a valuable object, etc. The video can be recovered from these events, and alerts and reports generated.

The analytics modules were designed to help surveillance and are not one 100% precise. For example: the missing objects module can create alerts if there are changes to the lighting, projected shadows, etc. and this creates the so-called false alarm.

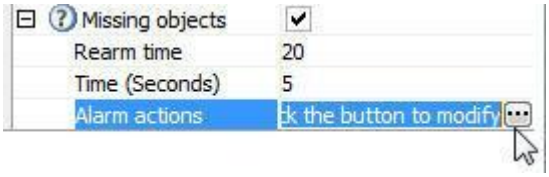
In our example, we created a detection area for an object on the table as in the picture below:

© 2002 - 2011 by Optiview USA all rights



As you can see in the Missing Objects, the zone must be delimited around a specific object, contrary to the Foreign Objects.
By opening the side options in **Missing Objects**, the following functionalities are available:

- **Missing Objects:** Tick this option to activate the Foreign Objects in this area.
- **Rearm time**: Rearm time for the alert to be activated again in the surveillance client (if configured).
- **Time**: Time in seconds the object must remain unmoving in the area to trigger the alert. Long periods are not recommended for areas where there is a lot of movement.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alert actions.

The following is an example of when the alert was triggered in the situation previously configured:

© 2002 - 2011 by Optiview USA all rights



Whenever an alert is triggered the scene is automatically captured.
To learn how to generate reports, refer to the Surveillance Client manual.

13.3.1.3 How to configure the Face Detection module

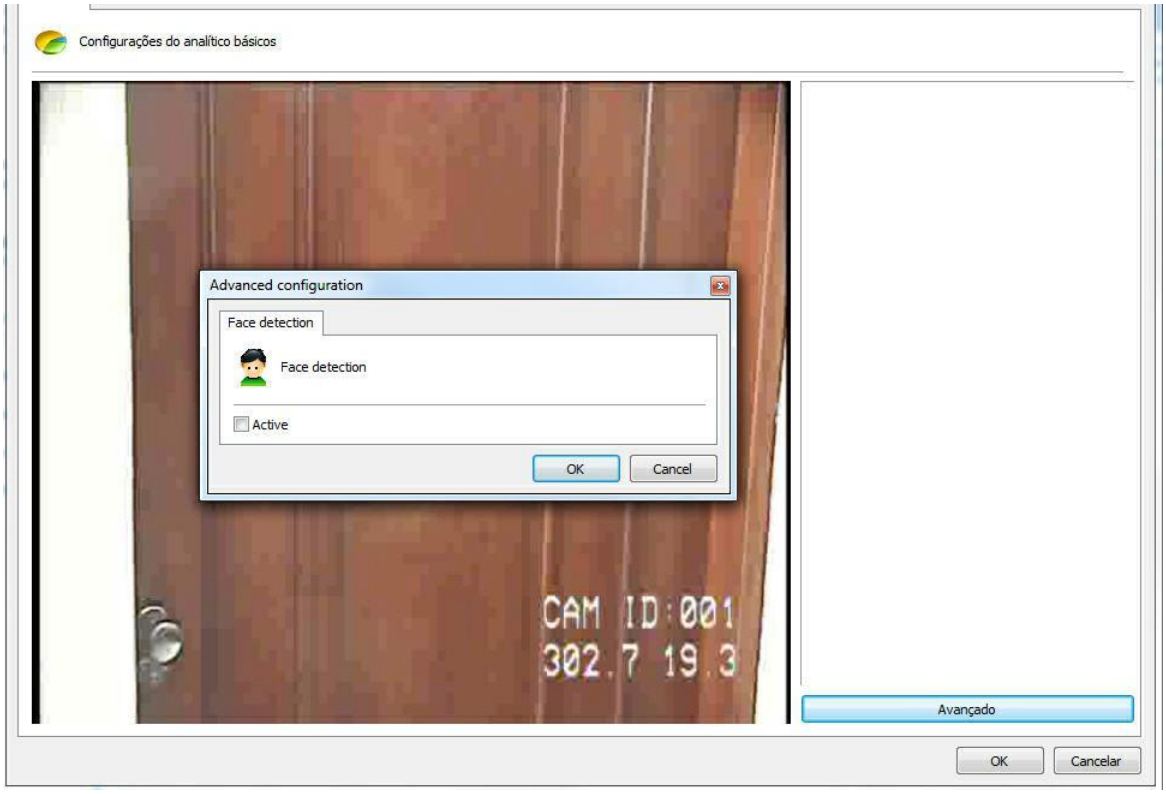
The aim of the **Face Detection** module is to capture the faces that pass by a certain camera and store them in a database.

For best results, the camera must focus a certain area so that the person's face occupies about 20% to 70% of the area of the image. Here is an example:

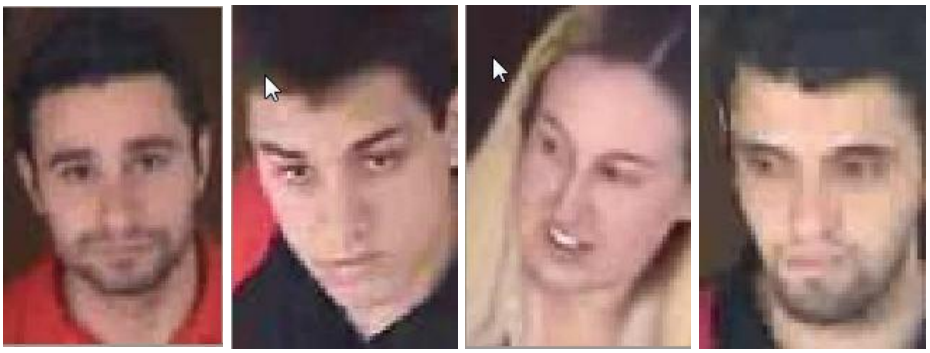


In the analytics configuration screen, click on the **Advanced** button and on **Activate** on face detection.

© 2002 - 2011 by Optiview USA all rights



The following is an example where the faces were captured in the situation previously configured:

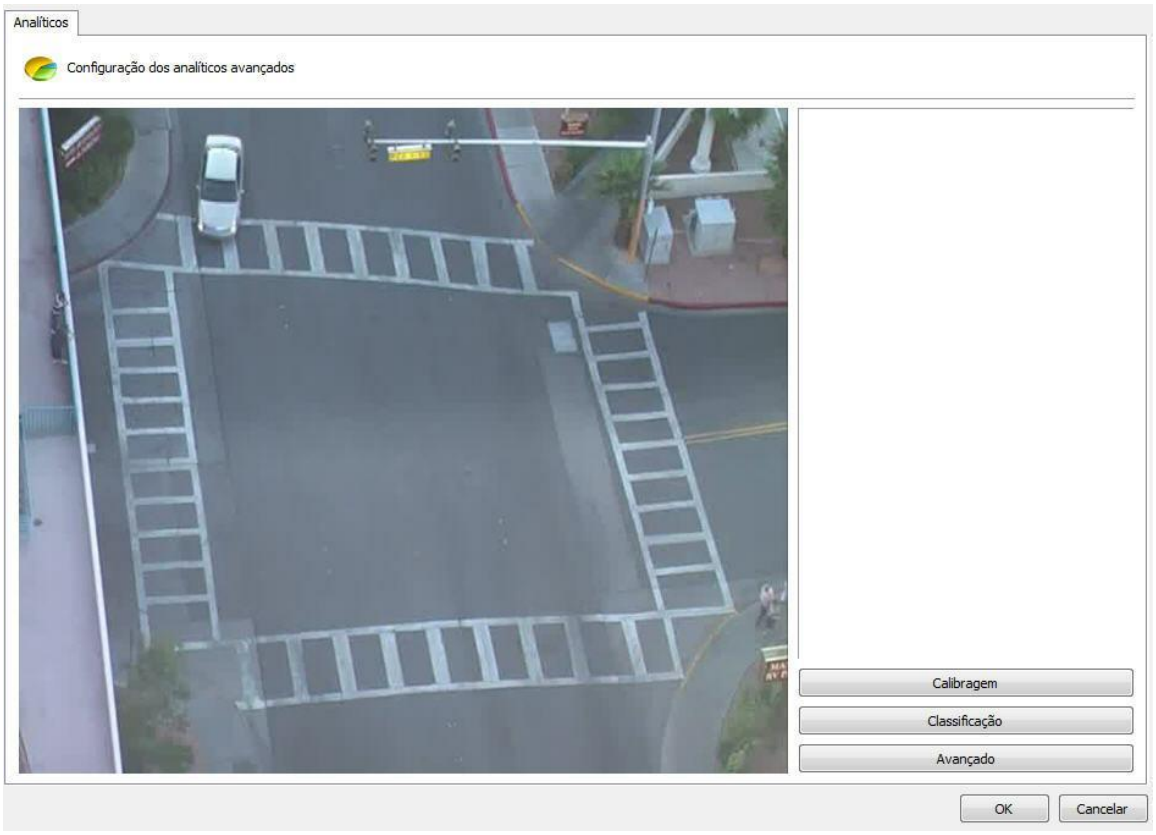


To learn how to generate reports and look up the faces captured, refer to the Surveillance Client manual.

13.3.2 How to configure the Advanced Analytics

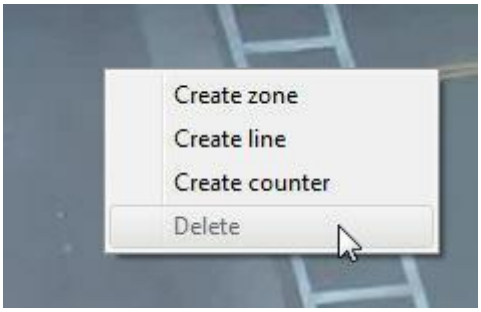
If the **Advanced** engine is chosen in the analytics register screen, the following screen will show up:

© 2002 - 2011 by Optiview USA all rights



The image that appears is related to the camera and the media profile selected in the register screen of the analytics.

This screen has the following functionalities when the right-hand button is activated:

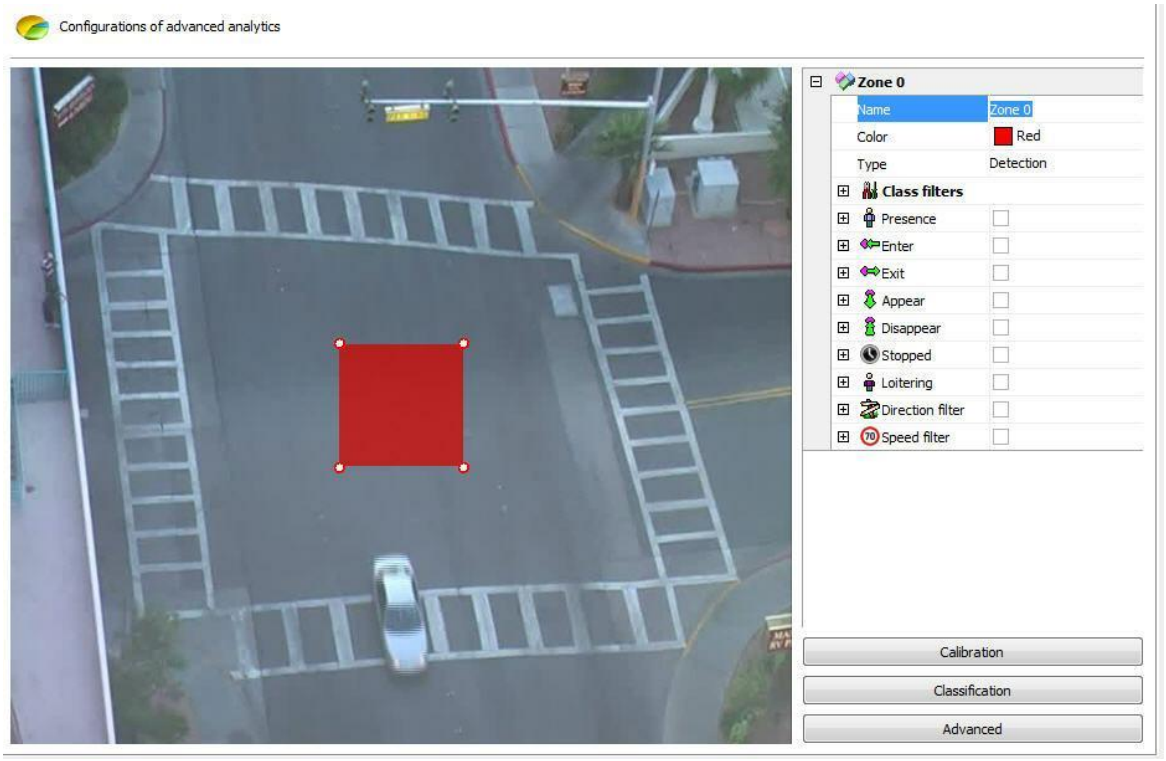


.

- **Create zone**: Creates a zone where the analysis module is defined (Rules).
- **Create line:** Creates a line where the analysis module is defined (Rule).
- **Create counter**: Creates a counter which will be associated to an analysis module (rule).
- **Delete**: Deletes a selected area/line/counter.

Create an area/line and click on it as shown in the picture below:

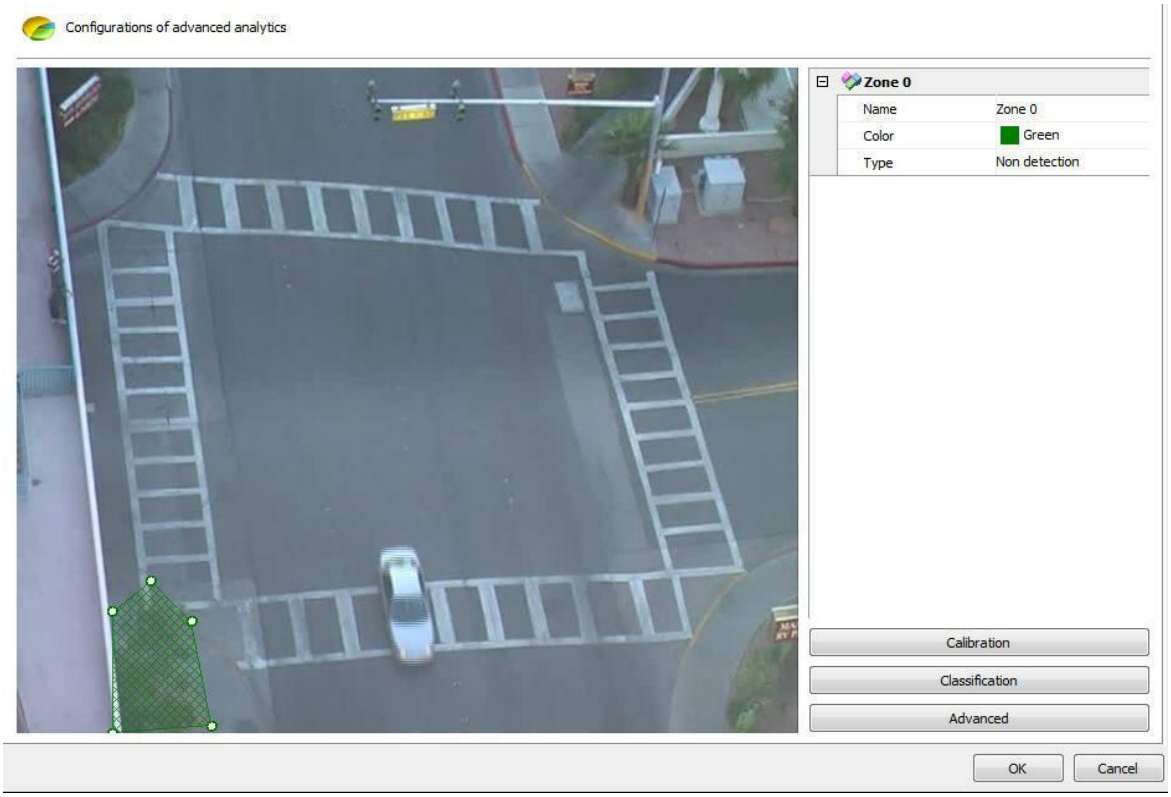
© 2002 - 2011 by Optiview USA all rights



An options menu of the area will open on the screen's right-hand column. The following options will be available:

- **Name**: Name for the area created. It is important to consider what name will be given as it will be possible to create reports using that name.
- **Colour**: Changes the colour of the area/line selected.
- **Type**: There are two area types: **Detection** and Non-detection.
  - The **detection** area is the standard area where the analytical modules are applied.
  - The non-detection area is used to remove unwanted areas from the image, such as trees, rivers, etc. The picture below illustrates a non-detection area:

© 2002 - 2011 by Optiview USA all rights



- **Object filters**: Determines the object that should be included in /excluded from the detection in the selected area. Learn more about this feature in chapter How to classify objects
- **Presence**: The module that detects the presence of an object within the selected area (person, cars, animals, etc). This module is described in chapter How to configure the Presence rule
- **Entry**: Module that detects when an object enters the selected area. This module is described in chapter How to configure the Entry rule
- **Exit**: Module that detects when an object exits the selected area. This module is described in chapter How to configure the Exit rule
- **Appear**: Module that detects when an object appears in the selected area. This module is described in chapter How to configure the Appear rule
- **Disappear**: Module that detects when an object disappears from the selected area. This module is described in chapter How to configure the Disappear rule
- **Stopped**: Module that detects when an object is unmoving within the selected area for more than a certain length of time. This module is described in chapter How to configure the Stopped rule
- **Loitering**: Module that detects when an object is moving within the selected area for more than a certain length of time. This module is described in chapter How to configure the Loitering rule
- **Direction Filter:** This module detects when an object is going through a wrong way. This module is described in chapter How to configure the Direction Filter rule
- **Speed Filter:** Module that triggers alerts when the speed of the object is between the configured maximum and minimum speeds. This module is described in chapter How to configure the Speed Filter rule

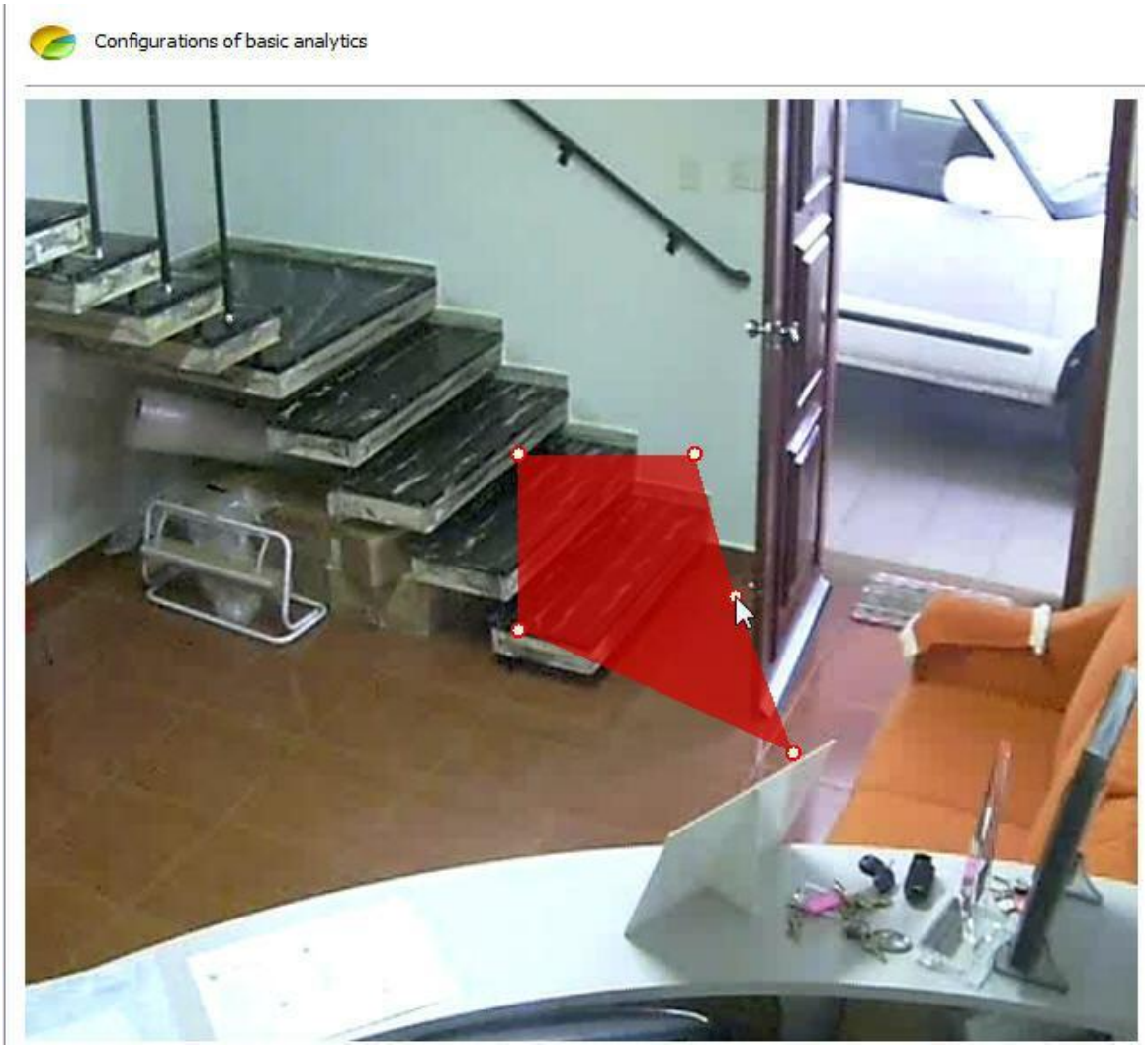
You can move the points in the area by clicking on the circles, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



And add points with a double-click near the area's edge as shown below:

© 2002 - 2011 by Optiview USA all rights



20 is the maximum number of points per area.
These same rules apply to lines.

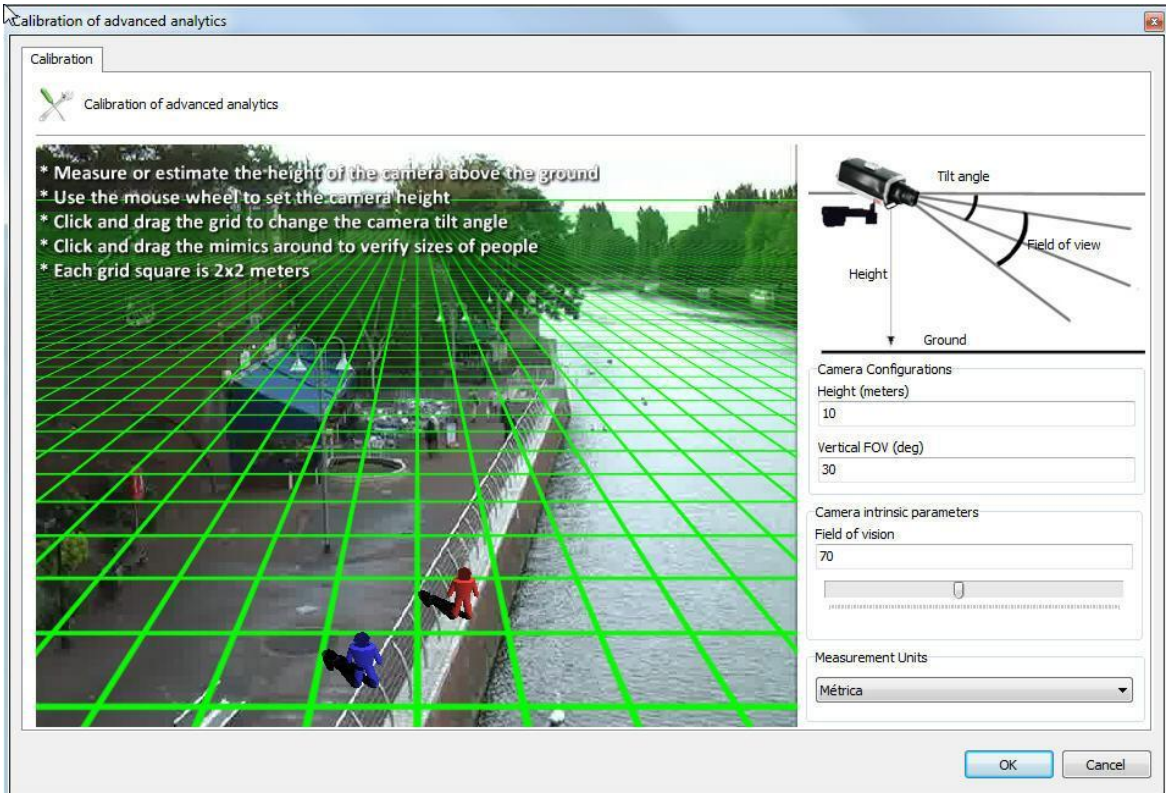
13.3.2.1 How to calibrate the analytics

The advanced analytics need to include calibration configurations so that it may operate suitably.

The first configuration is to calibrate the distances needed to get speed alerts and to classify objects such as cars, people, a group of people, etc.

To begin with, in the analytics configuration screen click on **Calibration**. The following screen will show up:

© 2002 - 2011 by Optiview USA all rights



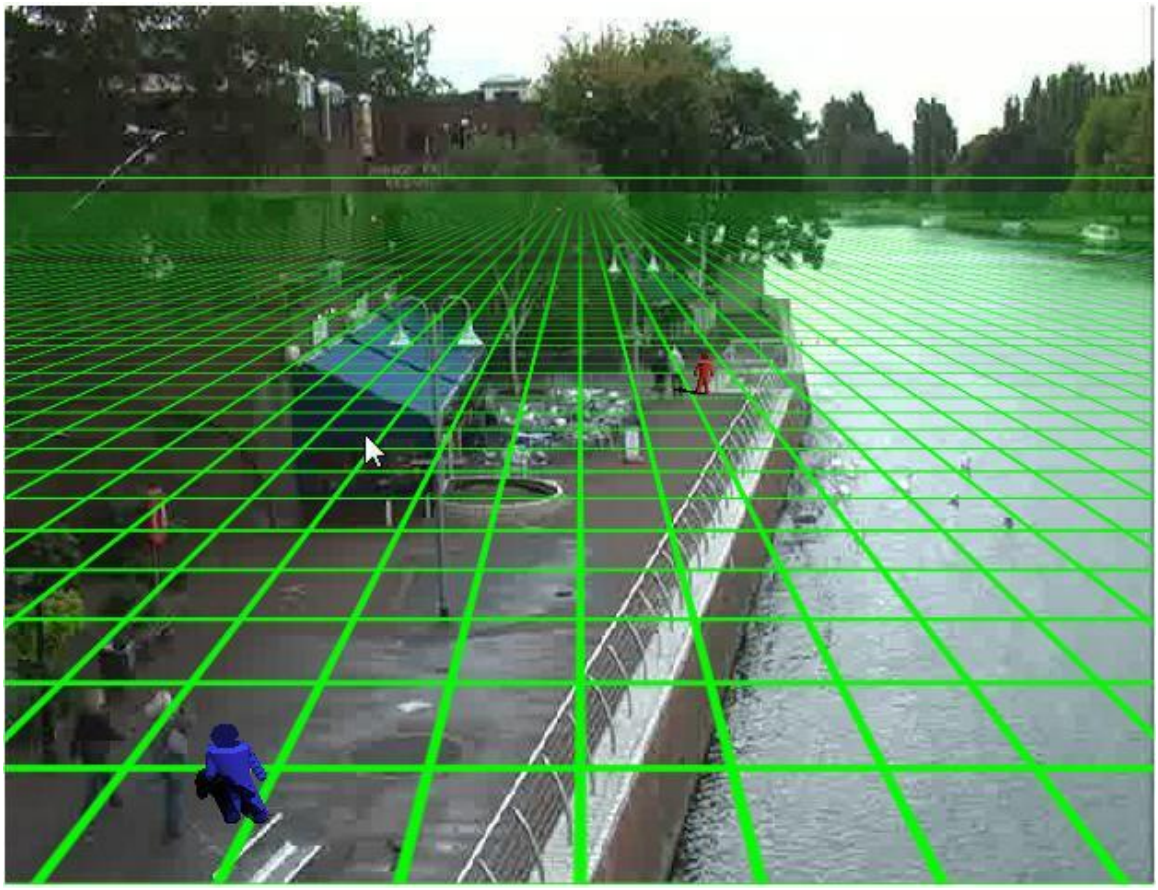
The image of the configured camera will appear in this screen as well as a 3DGrid.

If no command is activated, messages will appear on screen indicating how to operate the grid:

- Measure or estimate the distance between the camera and the ground.
- Use the wheel on the mouse to regulate the height of the camera.
- Click and drag the grid to change the vertical angle of the camera.
- Click and drag the 3D people to compare with the people on the image.
- Each square on the grid is equivalent to 2x2 metres.

For easier configuration, first move the grid so that the horizon line is compatible with the image, as shown in the picture below:

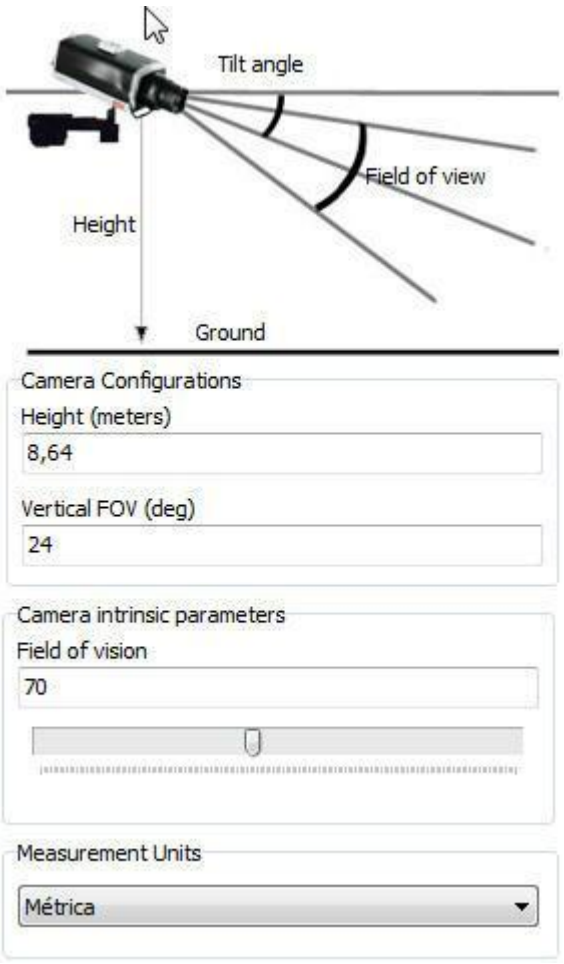
© 2002 - 2011 by Optiview USA all rights



In the configuration above you can see the line of the horizon on the grid compatible with the image, and the 3D figure with an approximate size to that of the people in the image.

Done! The grid is configured.
If you have precise measurements of the camera's position on site, the menu on the right can also help you configure the grid:

© 2002 - 2011 by Optiview USA all rights



The menu includes the following functionalities:

Height: The distance of the camera, in metres, to the ground.
Tilt Angle: Vertical angle of the camera.
Vertical FOV: Camera's field of vision.

If these figures are changed, the Grid's position is automatically altered.
It is also possible to change measurements from Meters to Imperial in the field Measurement Units.

With the grid correctly configured, you can classify the objects to be detected. For example: People between 2 to 3 metres tall walking at a speed of between 1km and 8km. Refer to the next chapter to learn how to classify objects.

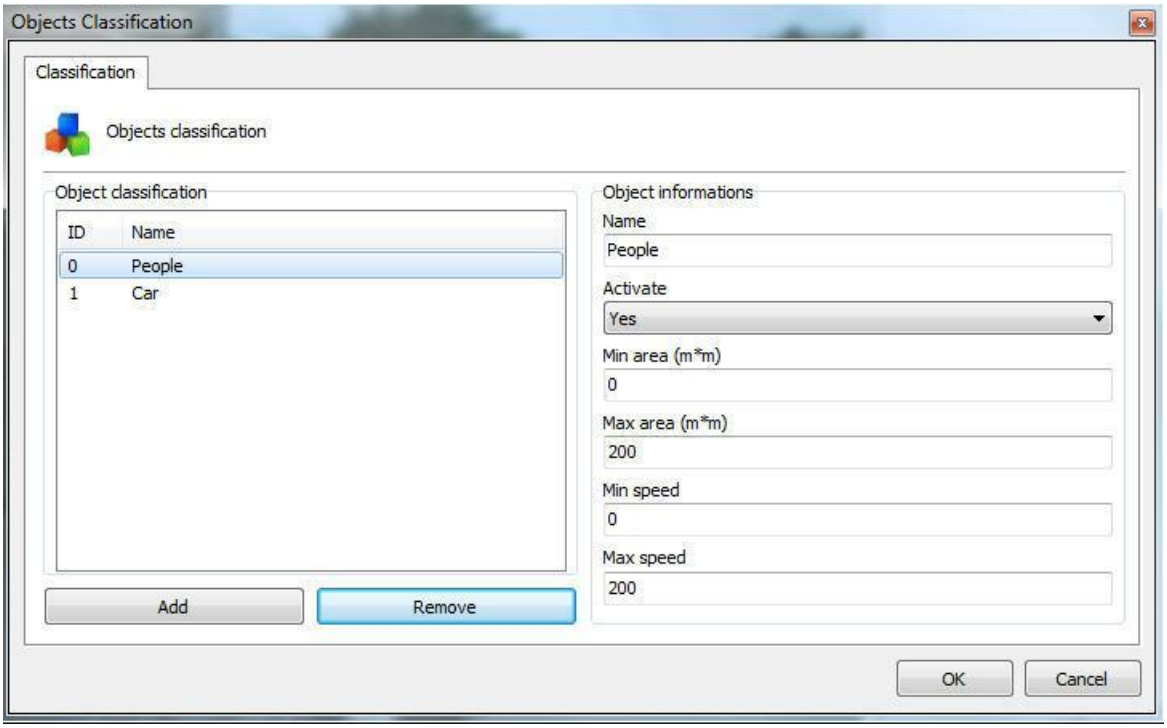
13.3.2.2 How to classify objects

The advanced analytics stores what type of objects triggered the alerts and filters them, for example, by cars, people, groups of people, animals, etc. Example: An area can trigger alerts only when there are people circulating or only when cars are motionless.

When the **Calibration** has been made correctly, you can create object classifications.

© 2002 - 2011 by Optiview USA all rights

To begin with, in the analytics configuration screen click on Classification. The following screen will show up:



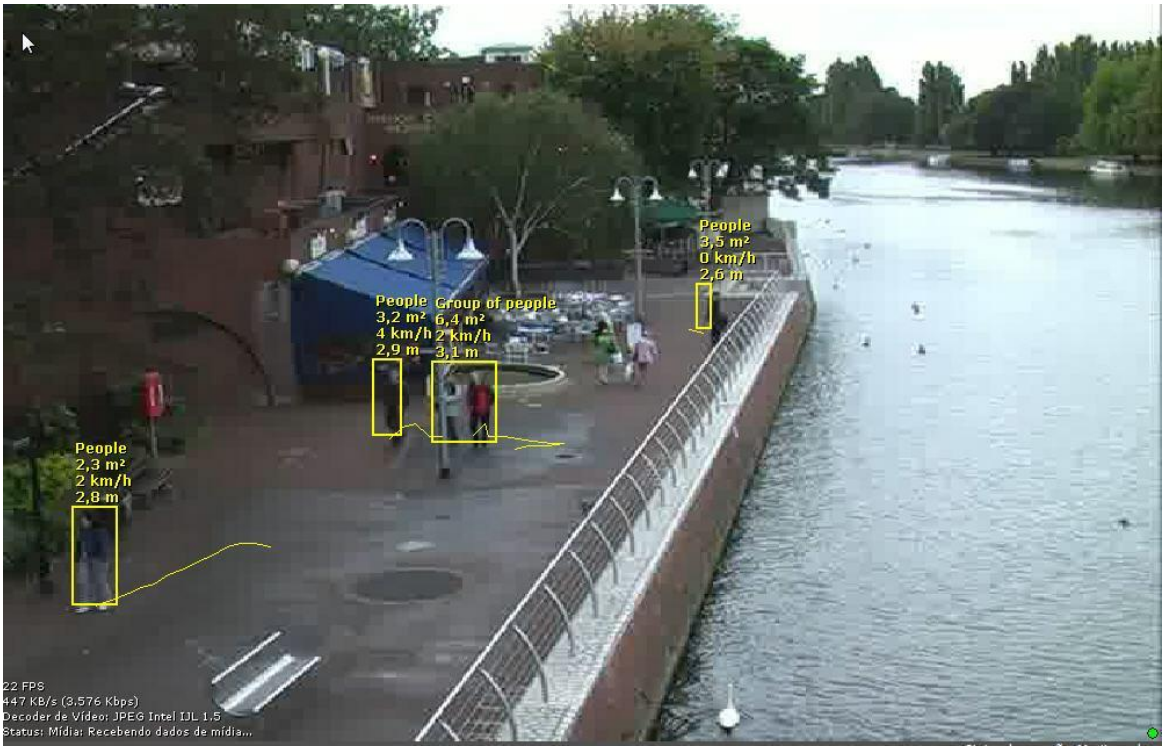
At first, there won't be any objects registered. To register an object, fill in the fields and click on Add. The picture above shows what the registration for "person" would be like.

The fields to be filled in are described below:

Name: Name of the classification to be added.
Activate: The classification can be deactivated at any given time; simply change the selection box to No.
Min. area: The minimum area the object must have to be recognized within that classification.
Max. area: The maximum area the object must have to be recognized within that classification.
Min. area: The minimum area the object must have to be recognized within that classification.
Max. area: The maximum area the object must have to be recognized within that classification.

To remove any classification, simply select it on the list and click on **Remove**.
Segue o resultado dessa classificação no monitoramento:

© 2002 - 2011 by Optiview USA all rights



To learn how to view the analytics' functionalities live, refer to the surveillance client.

13.3.2.3 How to configure the Analytics' Rules

Each analytics analysis module (Entry, Motionless, Presence) is considered a rule which, in turn, is applied to an area.

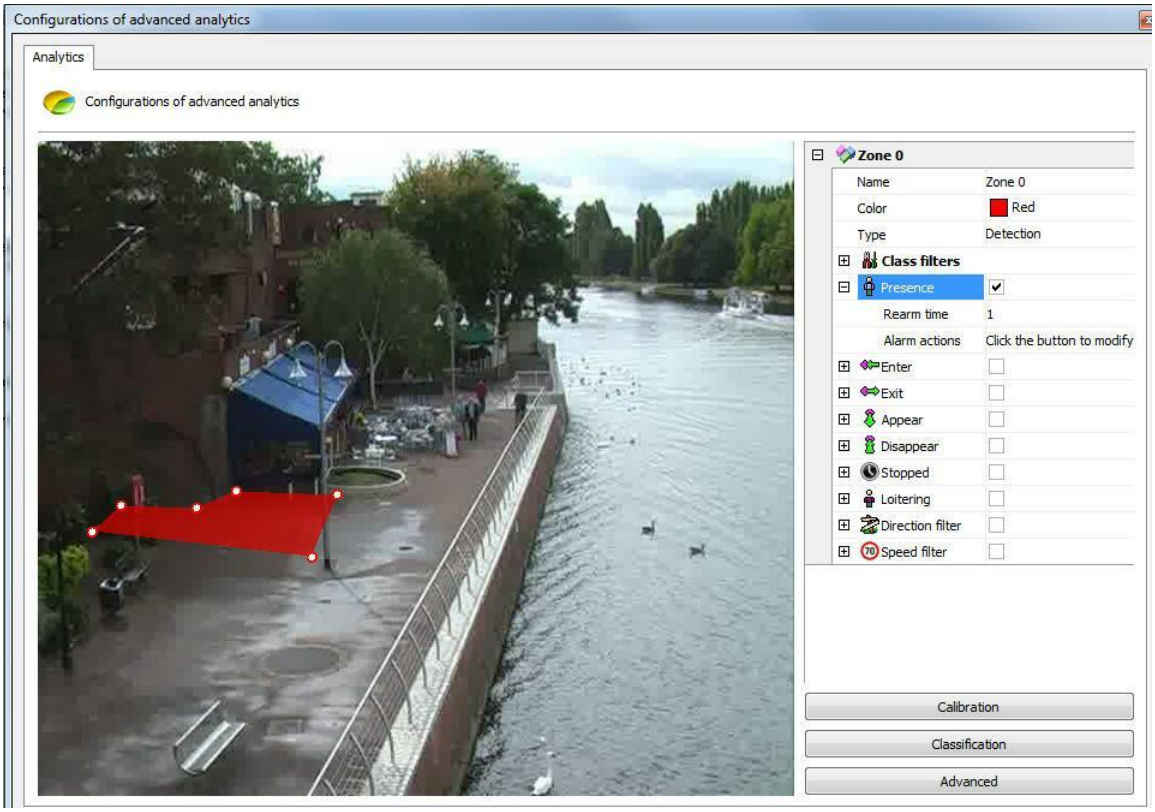
We will now see how to configure all the analytics rules and alerts in areas for different situations.

13.3.2.3.1 How to configure the Presence rule

The Presence rule can trigger an alert if it detects an object within a certain area.

Let's configure a presence alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2011 by Optiview USA all rights



With the area selected, click on Presence. The options for this rule are the following:

- **Rearm time:** Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:

In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alert actions.

Note

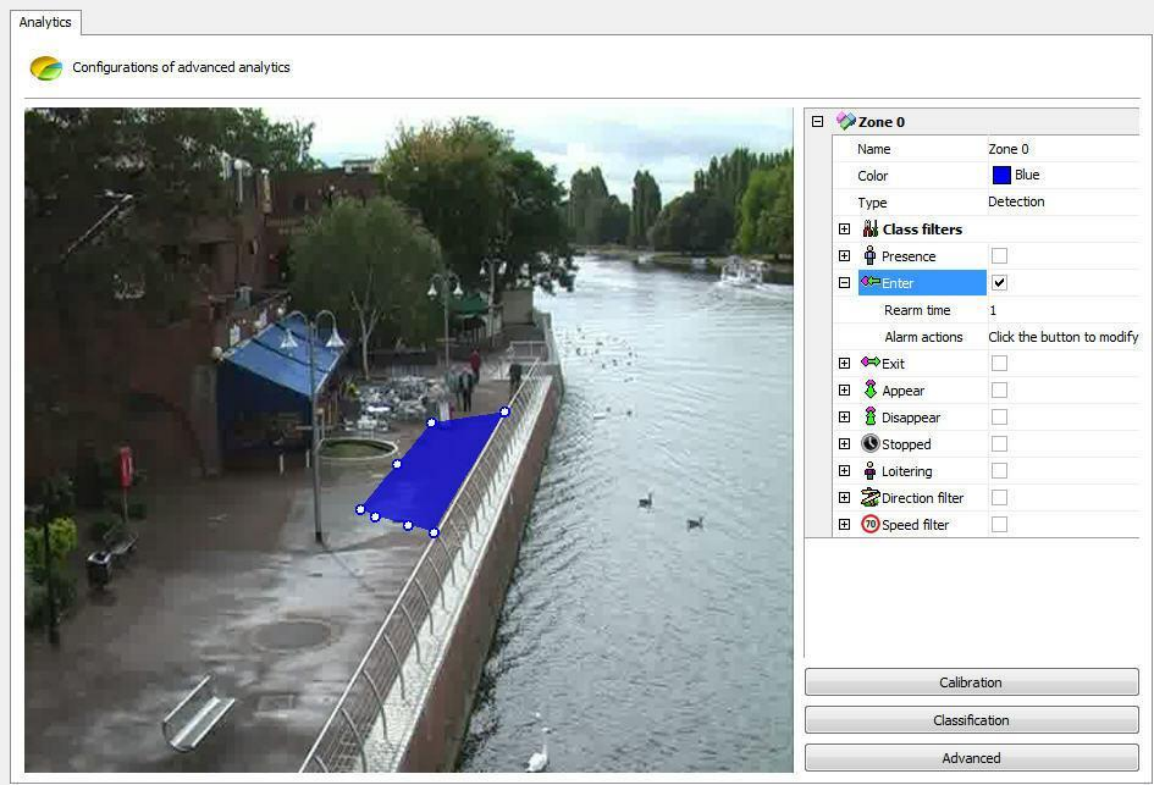
The presence rule indicates the number of objects detected within its area. The detected object can, for example, be 4 people standing close together and in that case the count info is 1 not 4.

13.3.2.3.2 How to configure the Entry rule

The **Enter** rule can trigger an alert if it detects an object entering a certain area.

Let's configure an **Enter** alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2011 by Optiview USA all rights



With the area selected, click on **Enter**. The options for this rule are the following:

- **Rearm time**: Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



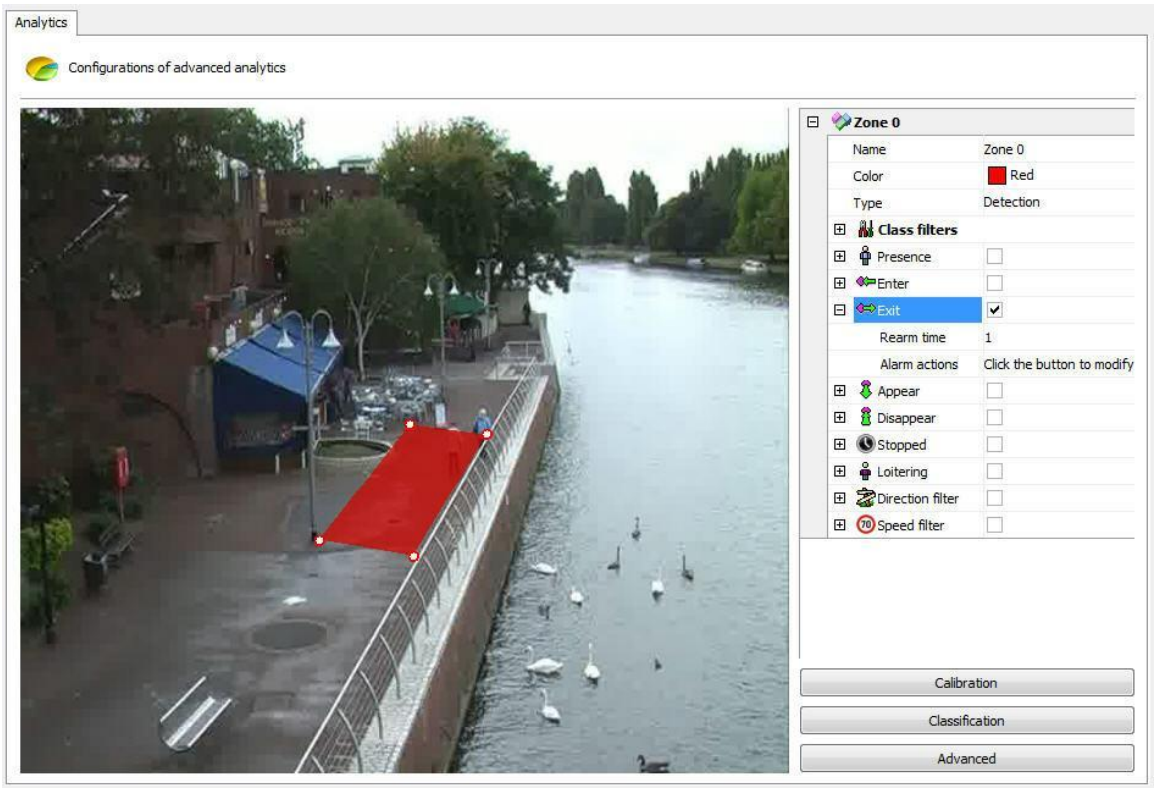
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

13.3.2.3.3 How to configure the Exit rule

The **Exit** rule can trigger an alert if it detects an object leaving a certain area.

Let's configure an **Exit** alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2011 by Optiview USA all rights



With the area selected, click on Exit. The options for this rule are the following:

- **Rearm time:** Time after which the alert actions are reactivated following an activity.
- **Alert Actions:** Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



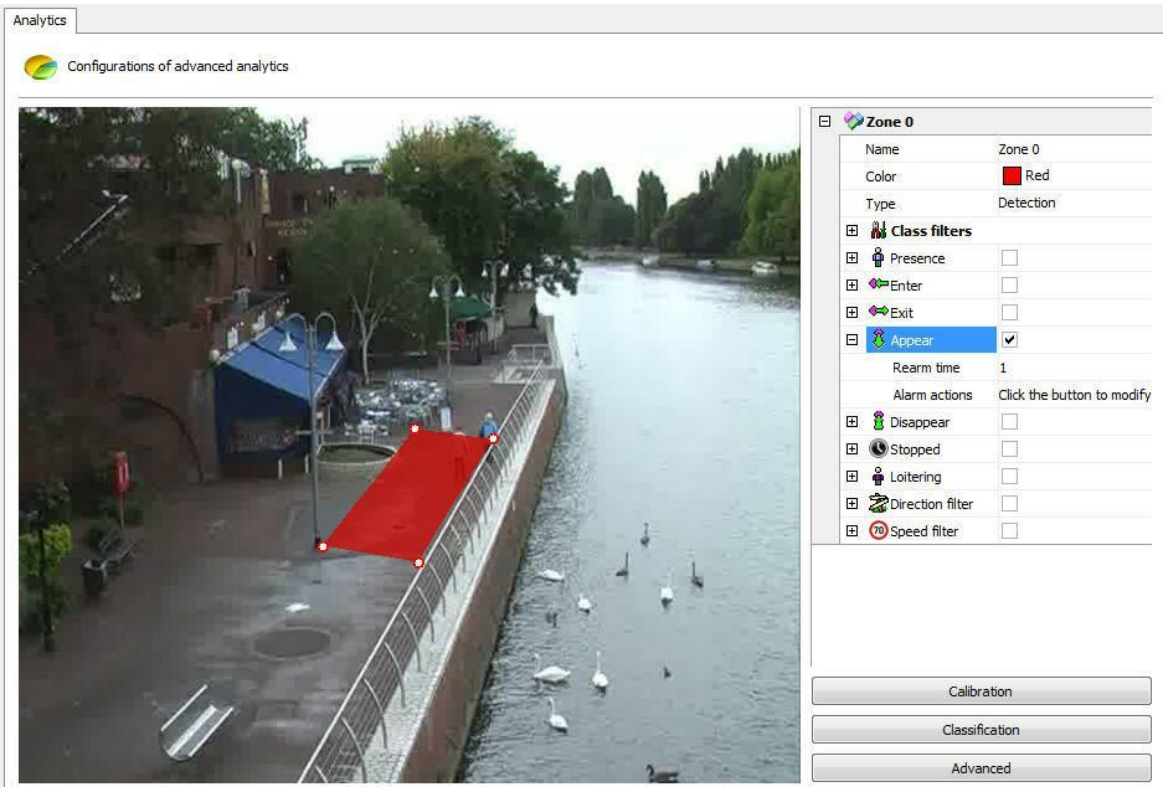
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

13.3.2.3.4 How to configure the Appear rule

The **Appear** rule can trigger an alert if it detects an object appearing in a certain area.

Let's configure an **Appear** alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2011 by Optiview USA all rights



With the area selected, click on **Appear**. The options for this rule are the following:

- **Rearm time**: Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



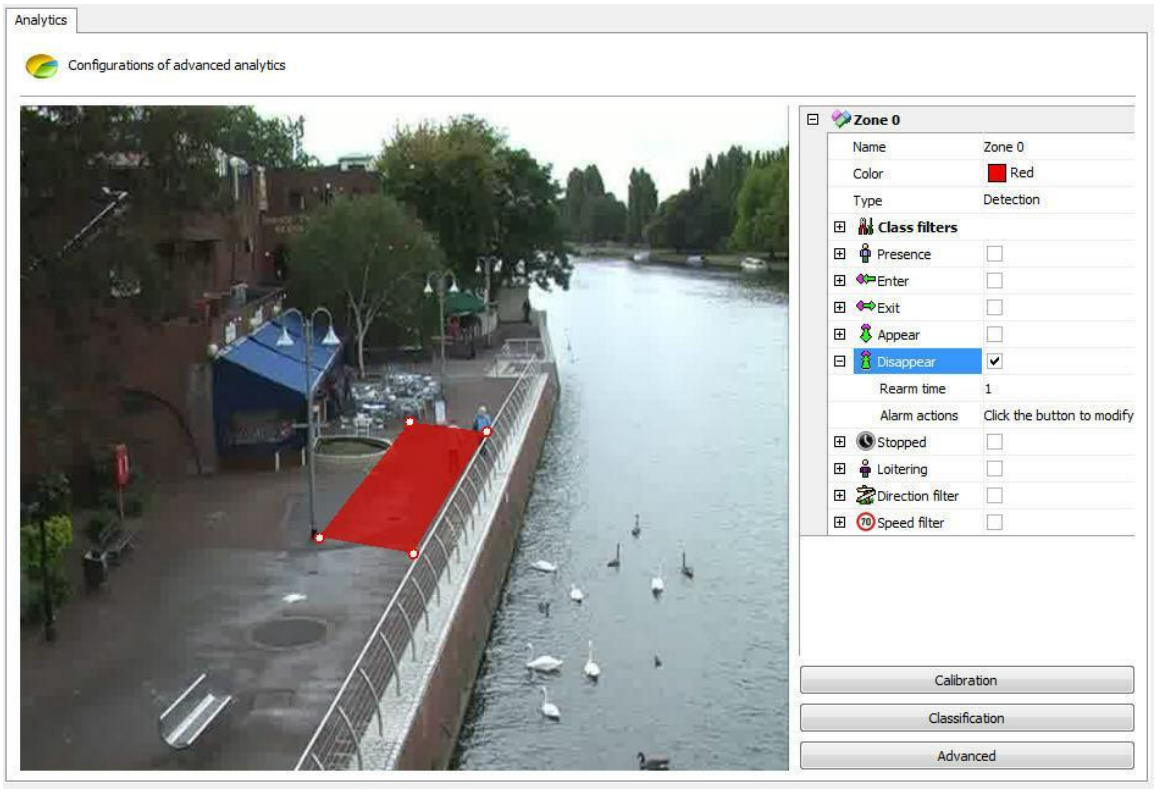
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

13.3.2.3.5 How to configure the Disappear rule

The **Disappear** rule can trigger an alert if it detects an object disappearing from a certain area.

Let's configure a **Disappear** alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2011 by Optiview USA all rights



With the area selected, click on **Disappear**. The options for this rule are the following:

- **Rearm time:** Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



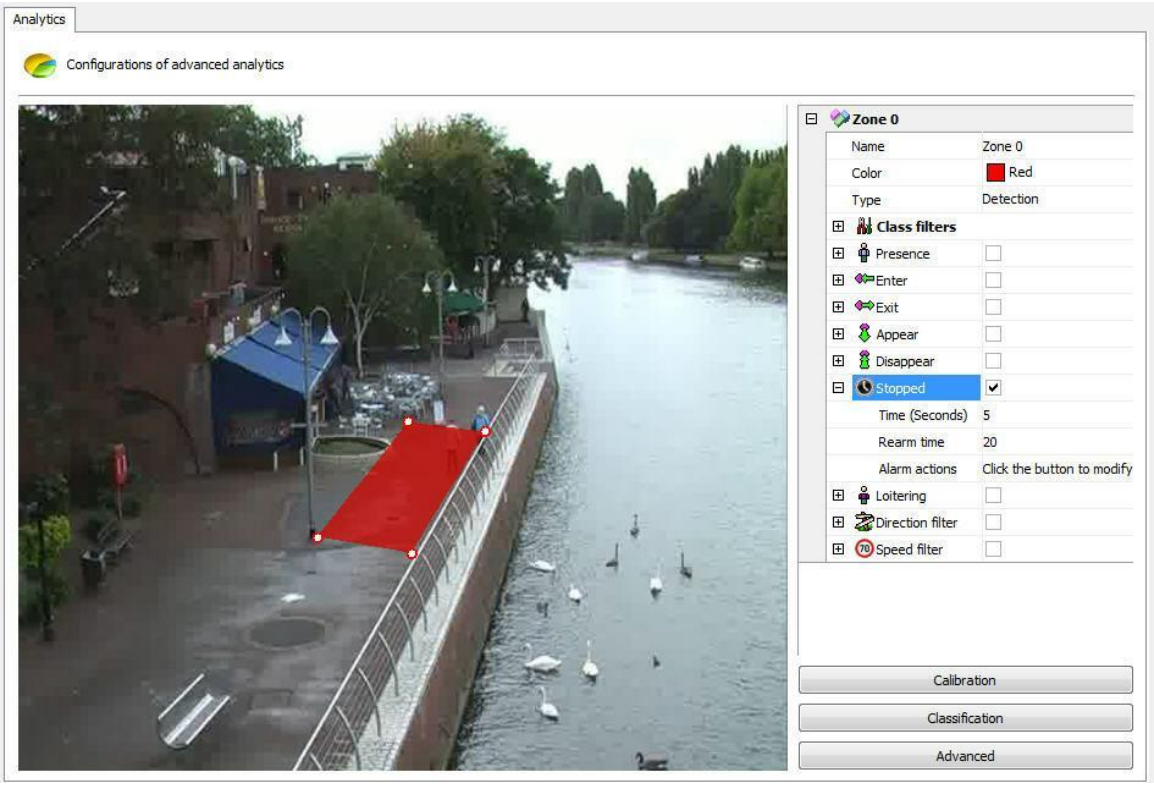
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

13.3.2.3.6 How to configure the Stopped rule

The **Stopped** rule can trigger an alert if it detects a motionless object in a certain area.

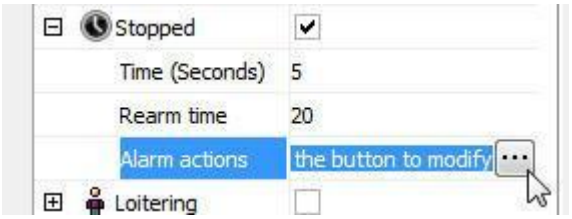
Let's configure a **Stopped** alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2011 by Optiview USA all rights



With the area selected, click on Motionless. The options for this rule are the following:

- **Time**: Time the object has to remain motionless to trigger the alert.
- **Rearm time:** Time after which the alert actions are reactivated following an activity.
- **Alert Actions:** Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



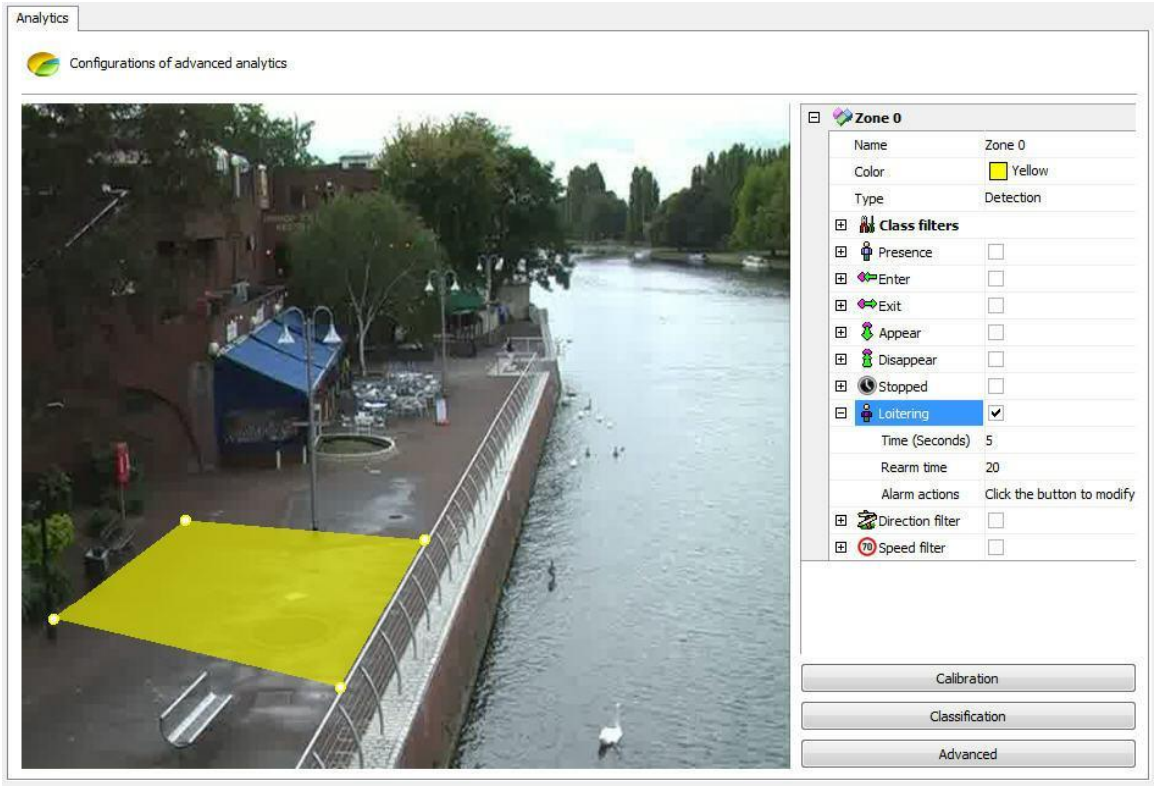
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

13.3.2.3.7 How to configure the Loitering rule

The **Loitering** rule can trigger an alert if it detects an object moving in a certain area for a certain amount of time.

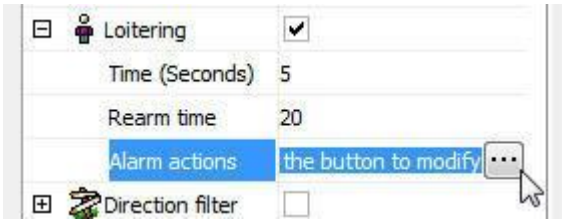
Let's configure a **Loitering** alert for a certain area. An area has been created in the previously calibrated image:

© 2002 - 2011 by Optiview USA all rights



With the area selected, click on **Loitering**. The options for this rule are the following:

- **Time**: Time the object has to remain motionless to trigger the alert.
- **Rearm time**: Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



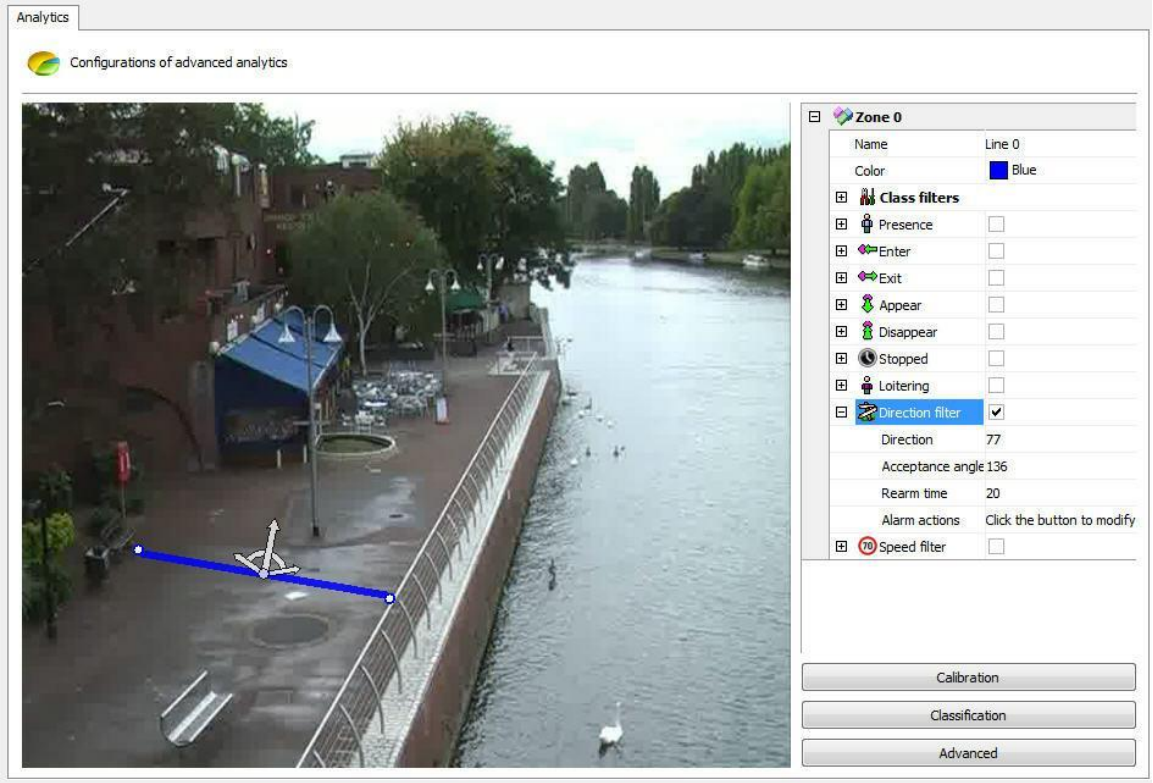
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

13.3.2.3.8 How to configure the Direction Filter rule

The **Direction Filter** rule can trigger alerts if it detects objects in configured directions.

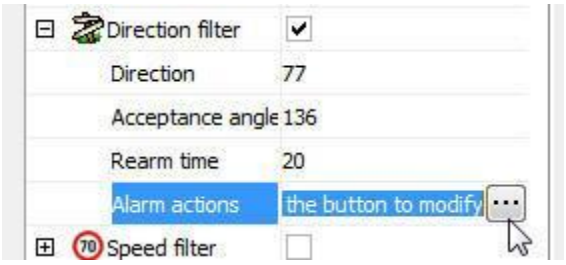
Let's configure a **Direction Filter** alert from a line. A line has been created in the previously calibrated image:

© 2002 - 2011 by Optiview USA all rights



With the line selected, click on the **Direction filter** rule. The options for this rule are the following:

- **Direction**: Direction within an angle in which the object must move along to trigger the alert.
- **Acceptable angle**: The acceptable angle is a slight difference from the main angle, that is, the object will not go past at exactly 90 degrees (it will pass at 100, 80, 70) so, the wider the acceptable angle, the easier it is for the alert to set off.
- **Rearm time**: Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



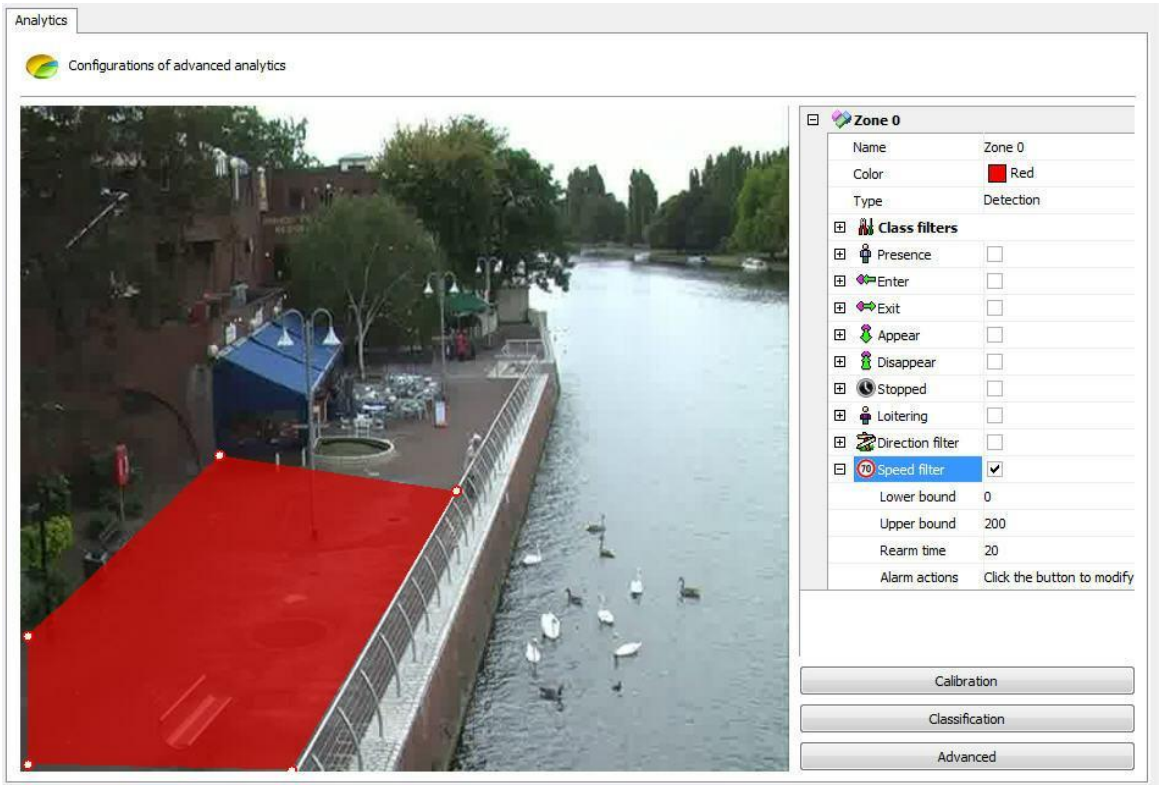
In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

13.3.2.3.9 How to configure the Speed Filter rule

The **Speed Filter** rule can trigger alerts if it detects objects at configured speeds.

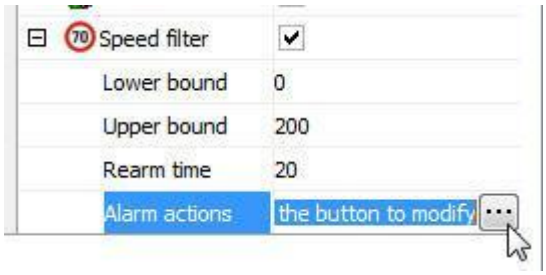
© 2002 - 2011 by Optiview USA all rights

Let's configure a **Speed Filter** alert from an area. An area has been created in the previously calibrated image:



With the area selected, click on the **Speed filter** rule. The options for this rule are the following:

- **Minimum Speed**: The minimum speed that the object must be moving to trigger the alert for that rule.
- **Maximum Speed:** The maximum speed that the object must be moving to trigger the alert for that rule.
- **Rearm time:** Time after which the alert actions are reactivated following an activity.
- **Alert Actions**: Click on the alert actions' line and then on the button with three dots, as shown in the picture below:



In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions.

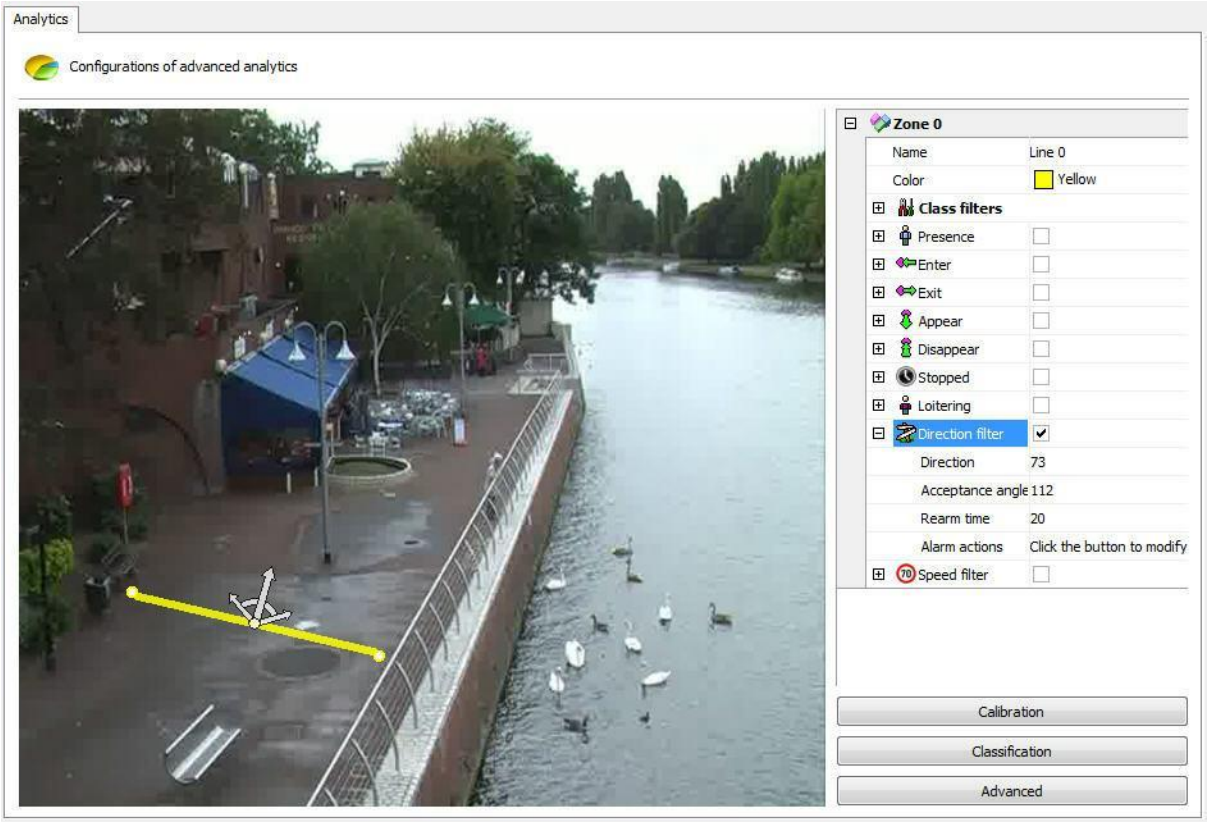
© 2002 - 2011 by Optiview USA all rights

13.3.2.4 How to configure the counters

The counters have visual objects that in real time allow to get information on the events taking place in the image surveillance.

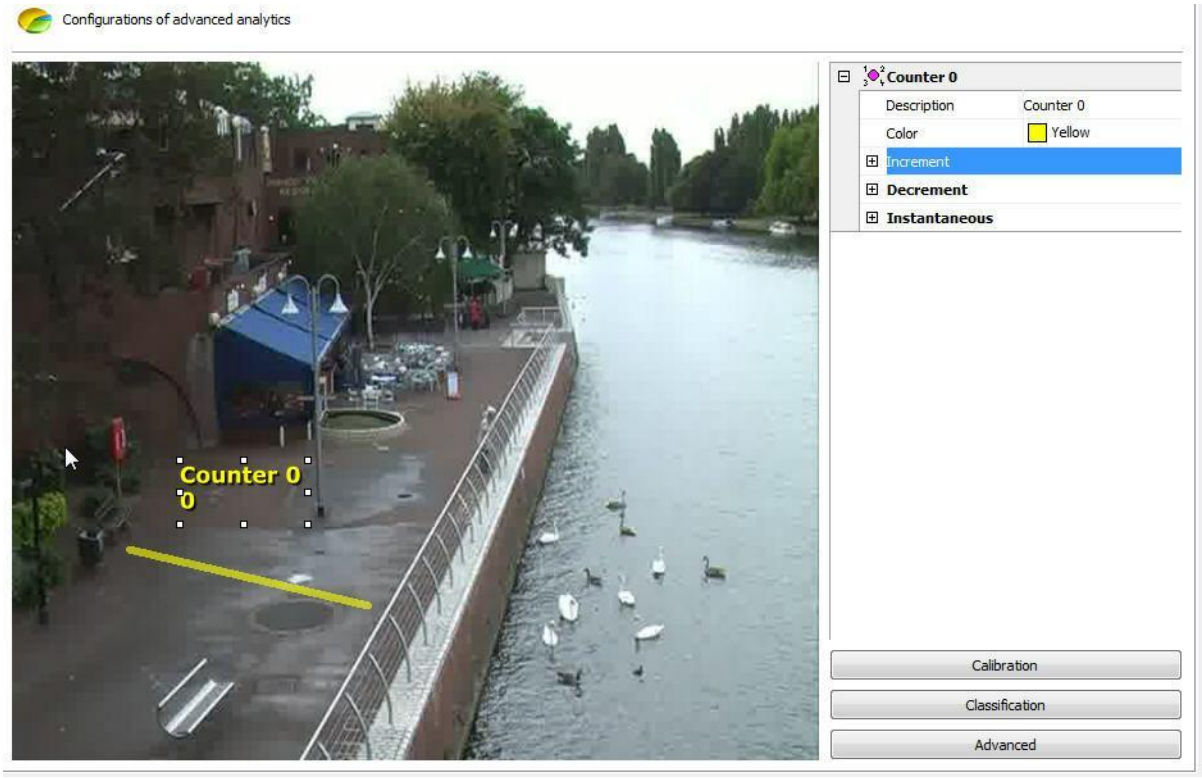
Counters are Incremented or Decremented by configured events. Let's see some examples.

In the picture below a Direction Filter rule has been configured.



We will configure a counter so that each object that activates this event will automatically be incremented by a counter. To do that, click with the right-hand button of the mouse on the screen and create a counter like the picture below:

© 2002 - 2011 by Optiview USA all rights

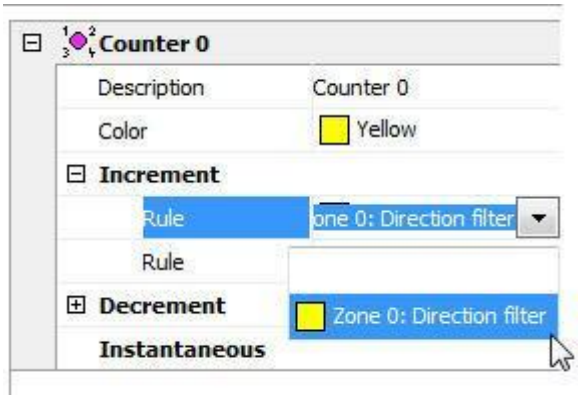


Some options are available in the menu on the right:

- **Increment:** Increments the counter according to the rules available.
- **Decrement:** Decrements the counter according to the rules available.
- **Instantaneous:** Returns the current value of the rules that are activated.

To understand better, let's see how to use the features above.

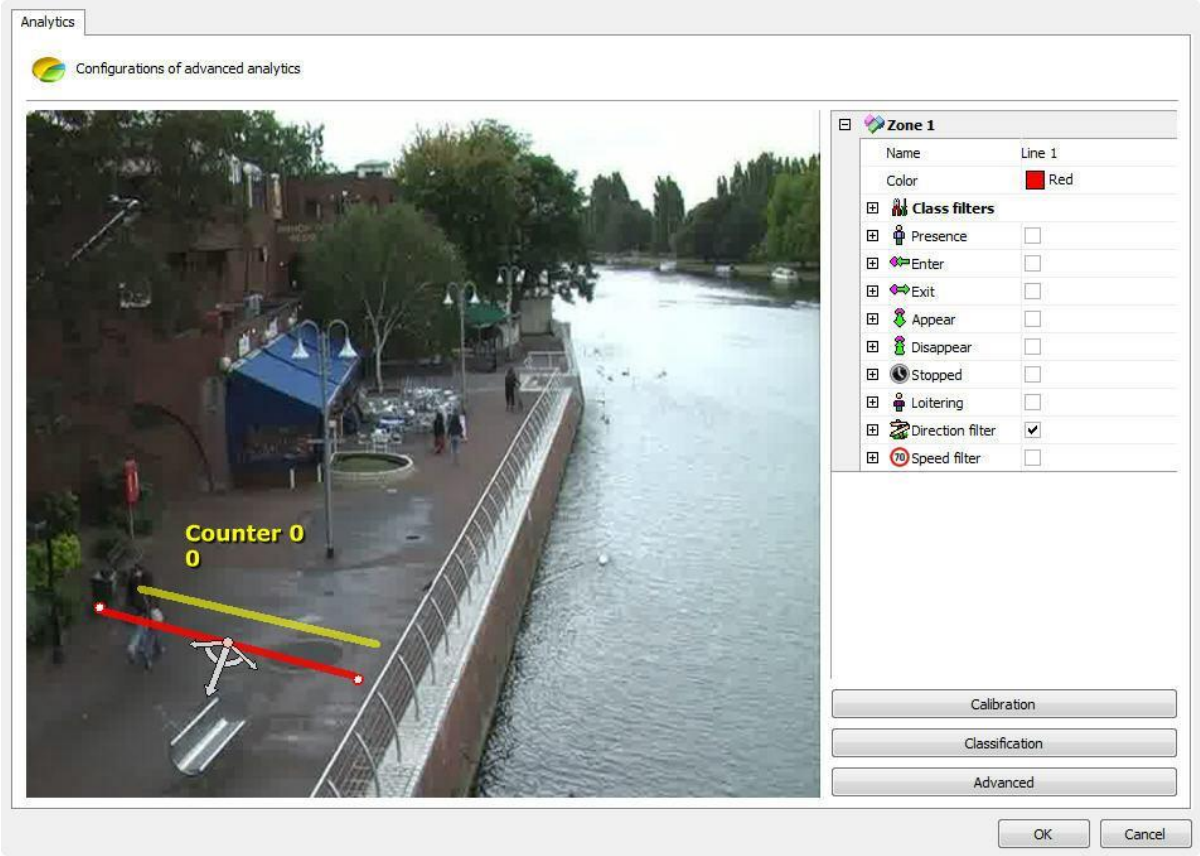
At first we will only increment the counter with direction rule that we created. To do that, open the **Increment** option and in Rule select the type of rule that you want to increment (in this case we only configured the Direction Filter, so it is the only one available).



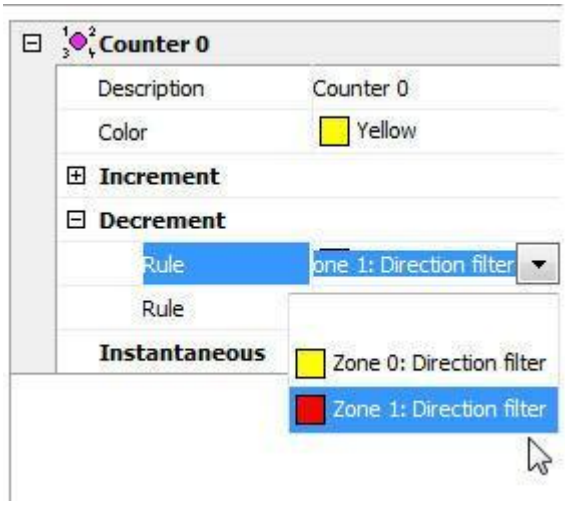
© 2002 - 2011 by Optiview USA all rights

When you select the rule you'll see that another **Rule** field will open and it could be used to apply another rule to increment the counter.

Now we'll create another **Direction Filter** field as shown in the picture below:



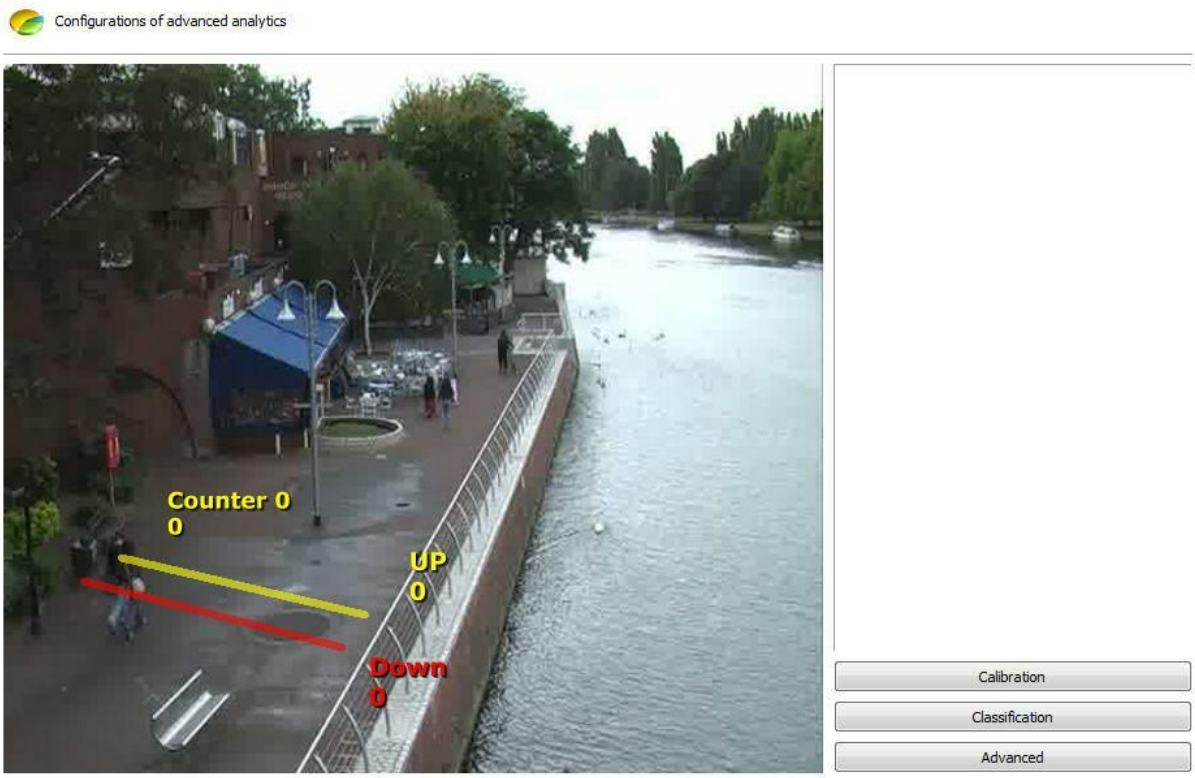
With that rule we'll **decrement** the counter already created.
Select it and in Decrement choose the rule of the second area as shown in the picture below:



© 2002 - 2011 by Optiview USA all rights

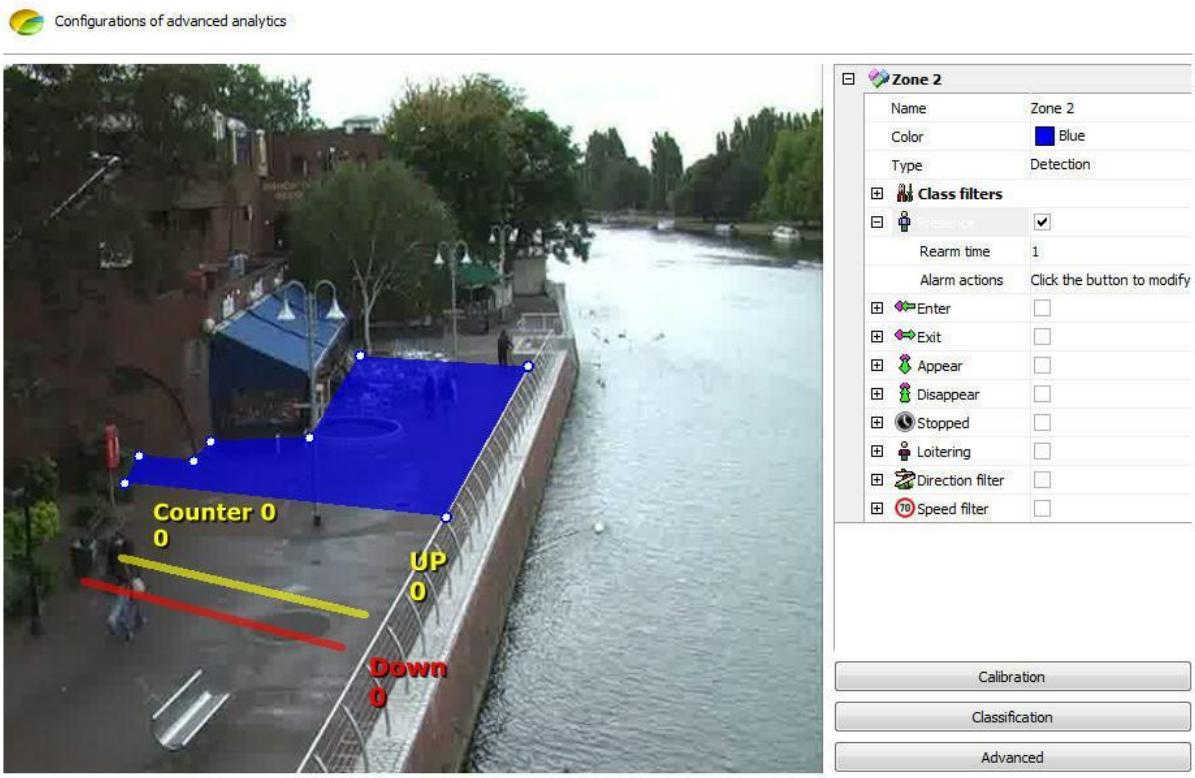
With this configuration, the Counter will **increment** when people walk up and **decrement** when people walk down.

There could still be a counter for each line as shown in the picture below:



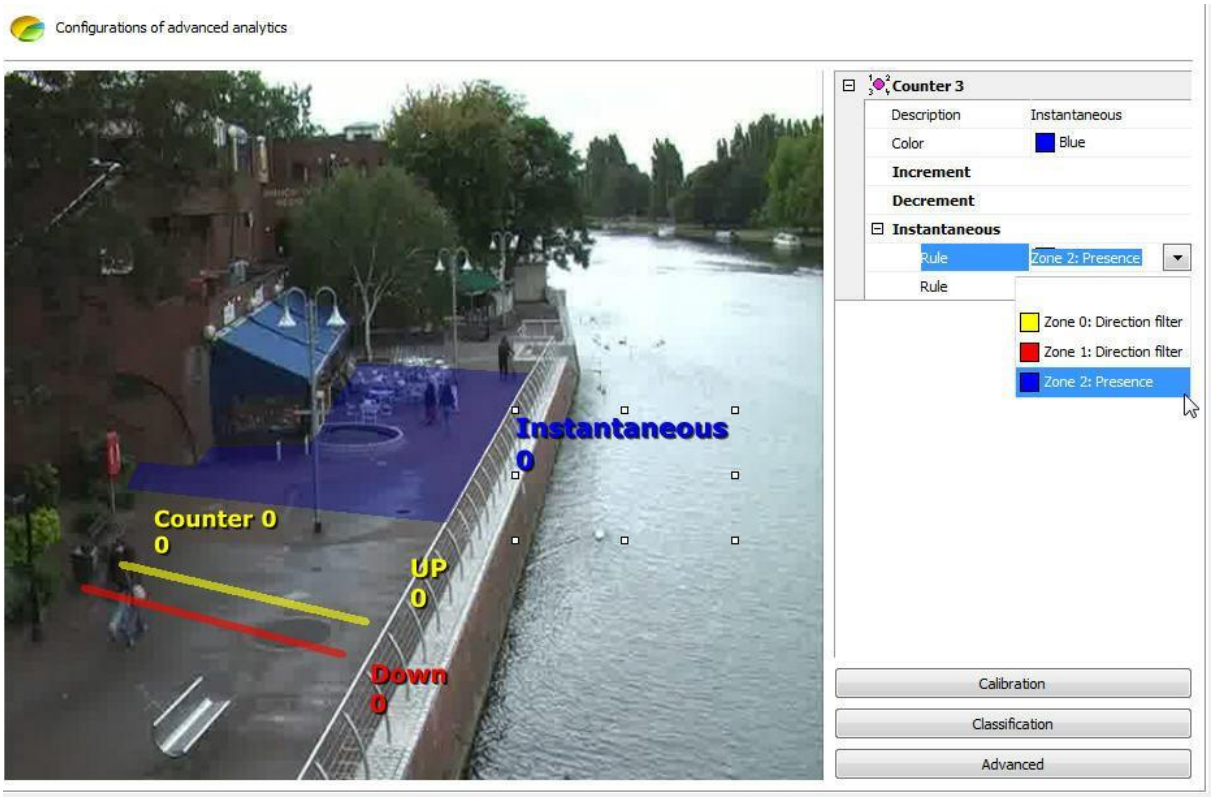
To test the instant counter we will create a presence detection area as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



Now a counter will be created to show the value of the presence rules activated within this area, in other words, it will give the number of objects present at the exact time within the area. The picture below shows that configuration:

© 2002 - 2011 by Optiview USA all rights



You can configure up to 40 counters per analytic configuration.
The counter size can be adjusted when selected and by dragging the squares around it.

13.3.2.5 The Analytics Advanced Options

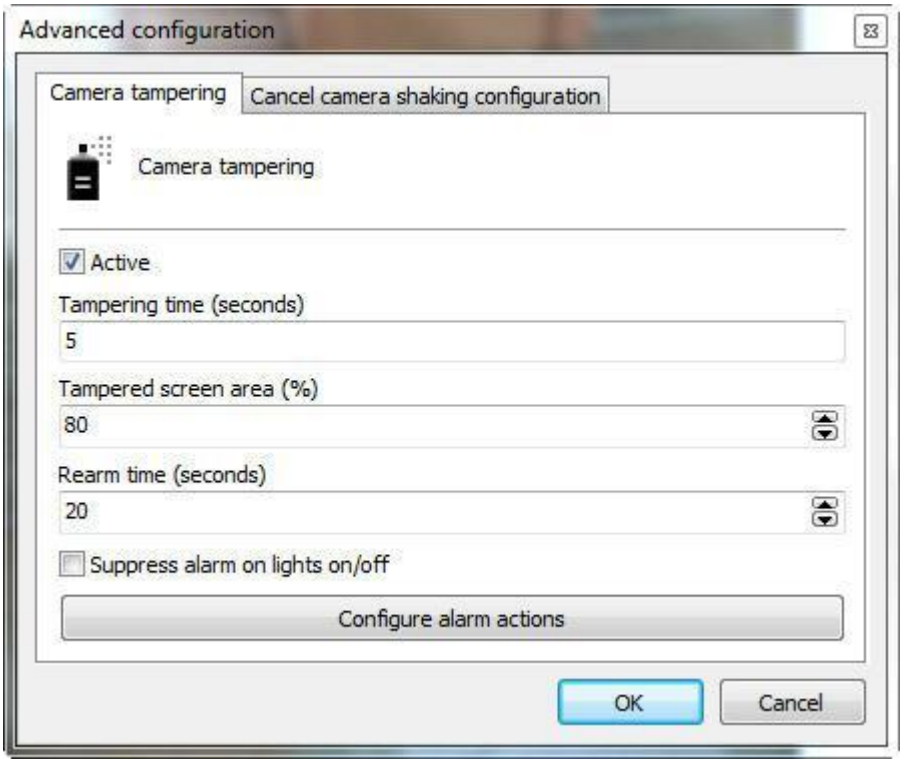
The advanced options include some general functionalities that will be described below.

13.3.2.5.1 How to configure the Camera Tampering

The Tampered Camera module can trigger alerts if there is something obstructing the camera, such as: the camera's position is altered, the lenses are fixed, an object is placed to block the view of a certain area.

To configure the tampered camera module click on the s button on the analytics configuration screen as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



This screen has the following functionalities:

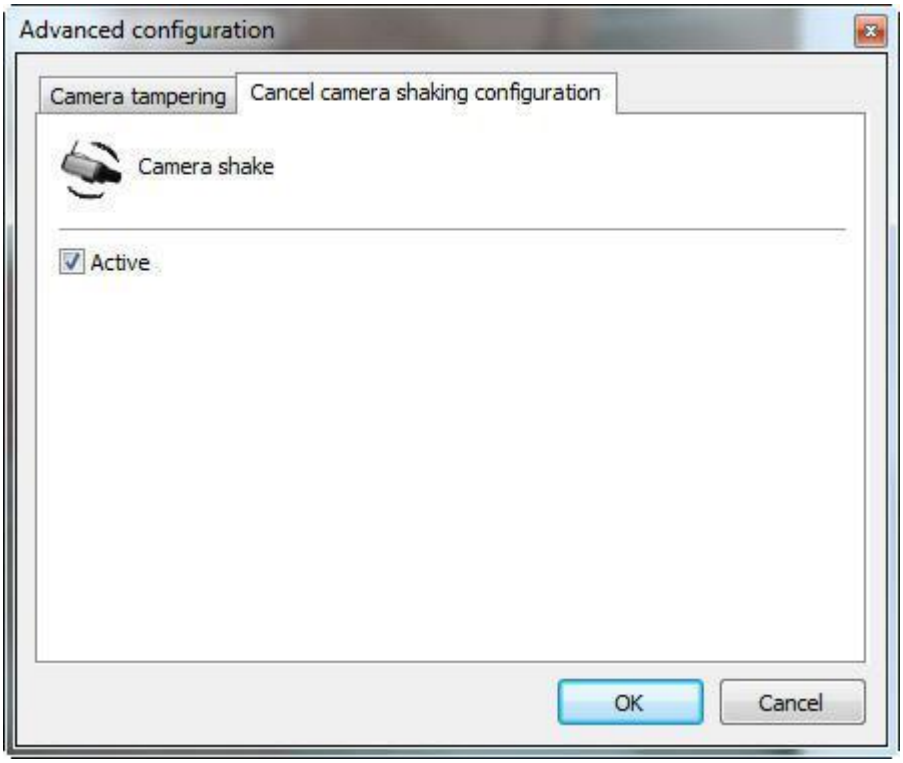
- **Activate**: Activates or deactivates the camera tampering module.
- **Tampering Time**: Time in seconds that the camera has to be obstructed to trigger the alert.
- **Tampered screen area**: Percentage of the image on the screen that must be obstructed to trigger the alert.
- **Rearm time:** Period before another alert is triggered.
- **Suppress alert on lights on/off**: The alert is not triggered if lights are switched on/off in the selected environment.
- **Configure alert actions:** In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alert actions.

13.3.2.5.2 Cancel Camera Shaking Configuration

The aim of this module is to help analyse images in cameras that may shake for several reasons. If the module is activated, it is much easier to analyse the image and there are lesser chances of mistake.

To configure the camera tampering module, click on the **Advanced** button on the analytics configuration screen and then open the tab **Cancel camera shaking configuration** as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



To activate the module, click on the **Activate** option as shown in the picture above.

© 2002 - 2011 by Optiview USA all rights

Chapter XIV

14 License Plate Recognition

The LPR server is a different module to the Digifort server, as well as the Analytics Digifort.

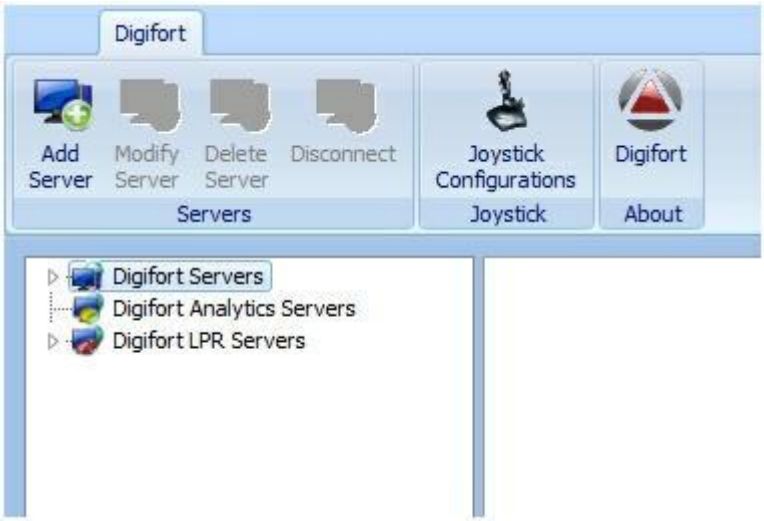
The LPR and Analytics servers are installed together with the Digifort server; however, the licenses are purchased separately.

The LPR works with two different engines: Kapta and Carmen. As well as the basic license which must be purchased so that they may work with Digifort, both engines work with a Hardkey, including the Digifort basic license.

The Kapta and Carmen engines work differently: Kapta is a national license and is licensed according to the number of cameras to be used by the server.
Carmen is an international engine and works with an unlimited number of cameras, its only limit being your computer's hardware.

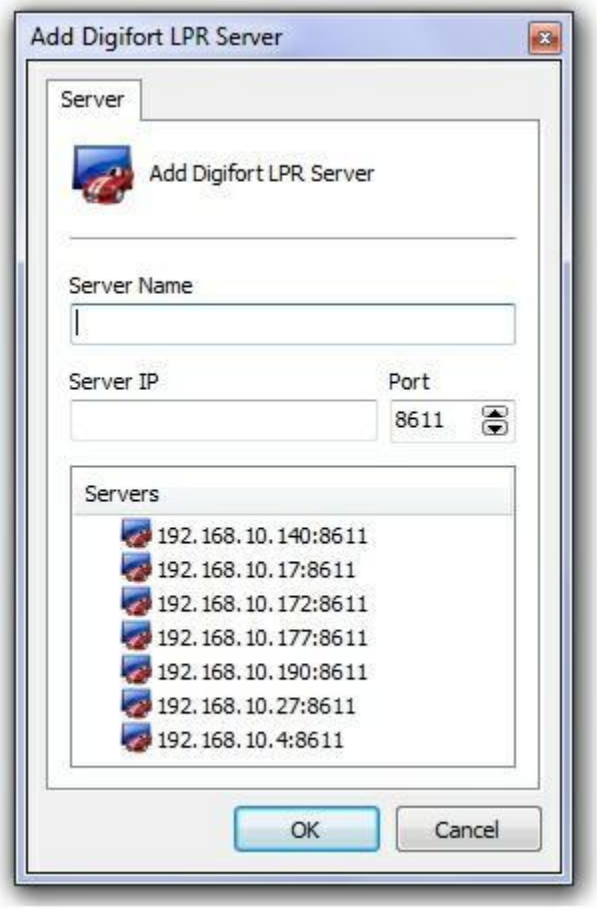
14.1 How to create a License Plate Recognition Server

To start using the LPR module, you must first create a Digifort LPR Server.
In the Administration Client, select the **Digifort LPR Servers** option and click on “Add server”, as in the picture below.



Select the “Digifort LPR Servers” option and click on the button **Add Server** on the top left-hand corner of the screen.
The following screen will show up:

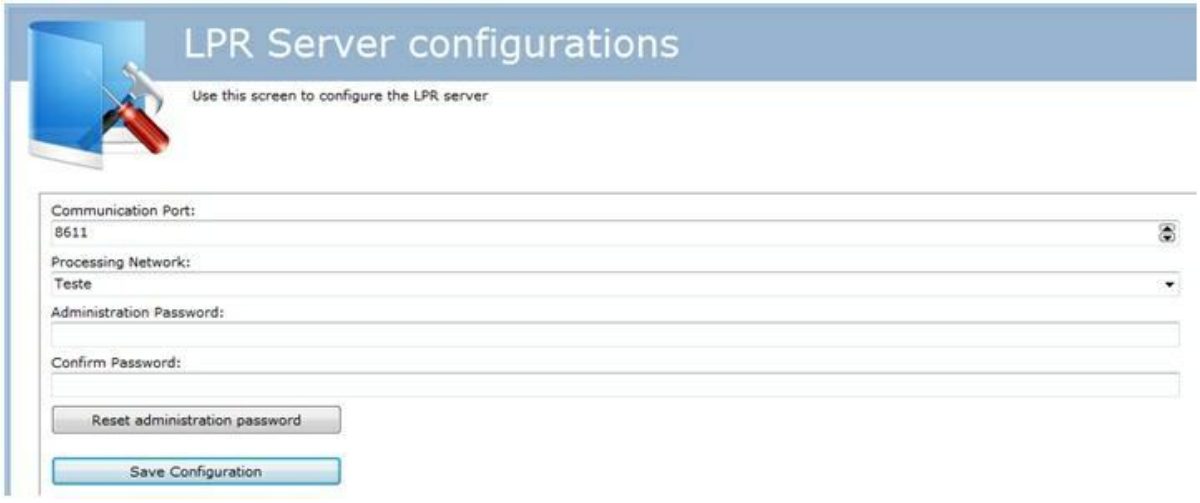
© 2002 - 2011 by Optiview USA all rights



In this screen you have to define a name and an IP where the LPR Server is active. When you've done this, click on **"OK"**.

14.1.1 How to configure your LPR server

As configurações do servidor LPR são bem simples como mostra a imagem abaixo:

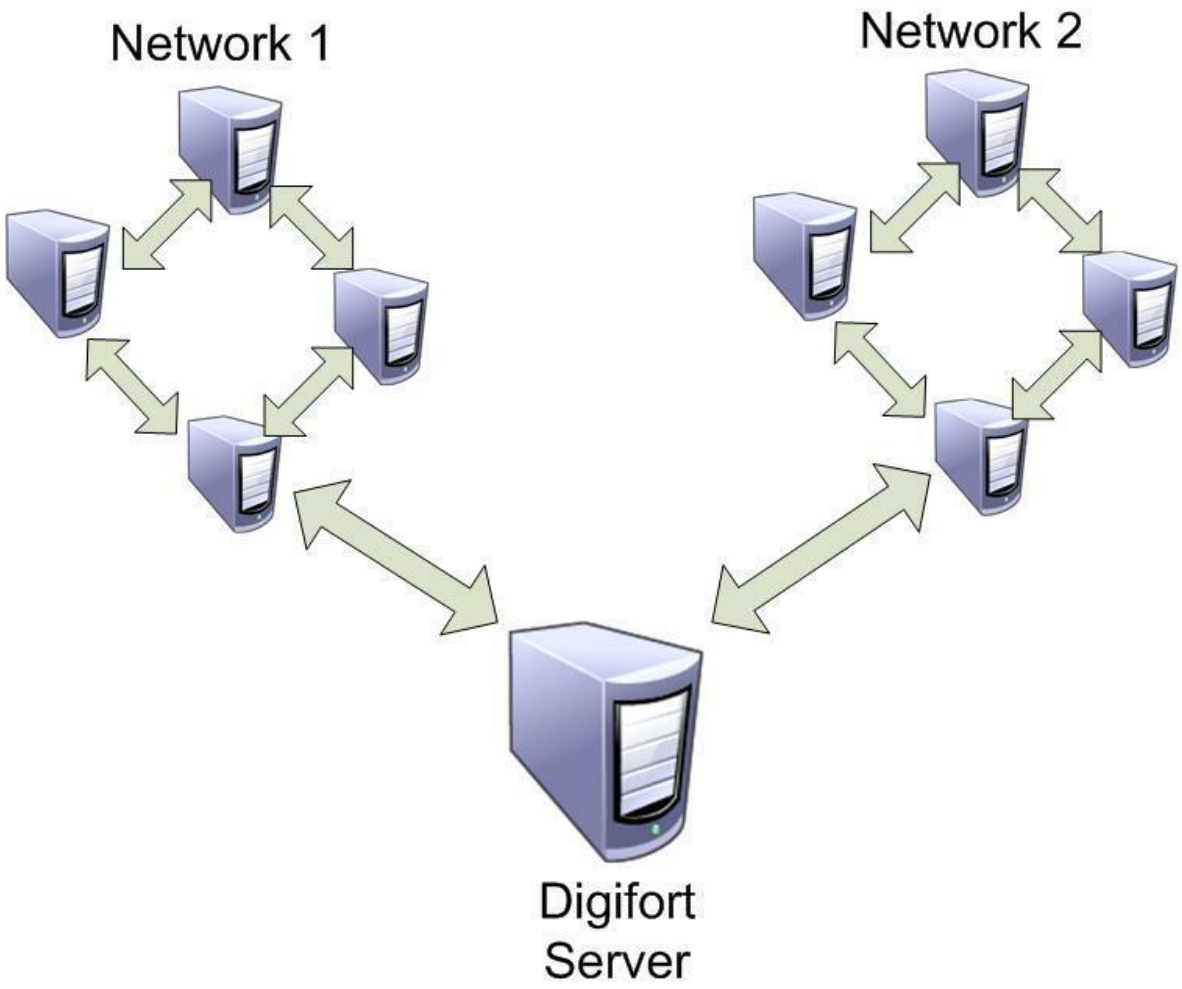


© 2002 - 2011 by Optiview USA all rights

The only configurations to be applied are:

- **Communication Port:** Communication port to the analytics server. It is recommended that you change this only if another program is already using it.

- **Processing Network:** Name of the distributed network where the server will counterbalance the load. When more than one server has the same "Processing Network" name there will be a processing counterbalance among them. Look at the diagram below to get a better idea:



In the picture above, the **"Digifort Server**" sends the images of the cameras to two different " **Processing networks**". This way, each set of computers only balances the load among the **LPR Servers** with the same network name.

- **Administration Password**: Password to access the analytics server. Fill in this field to change the current password.
- **Confirm Password**: Type the password again.
- **Save configurations**: Saves changes made on the screen.

© 2002 - 2011 by Optiview USA all rights

The default port is 8611, but it can also be edited.
The processing network can have any name chosen by the user who can also create an authentication password.

14.2 Licensing the LPR

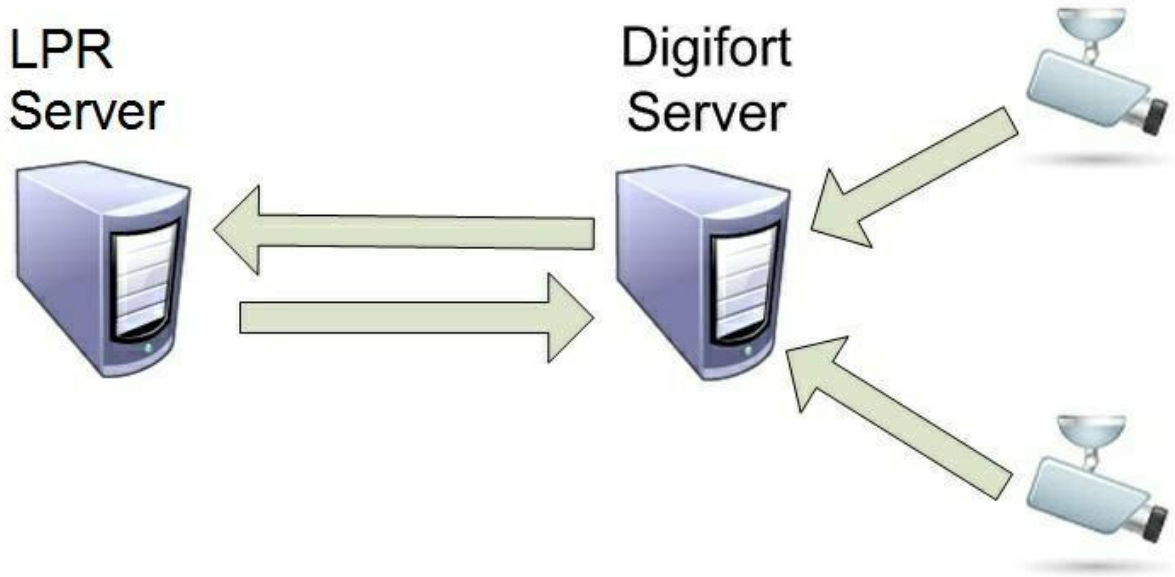
How does the architecture for the Digifort LPR work?

The license for the LPR server works like the server for the Digifort cameras, there is a “base license” for the server and other licenses for the LPR.

There are two types of licensing, one for **Kapta** engine and other to **Carmem** engine.

The **Kapta** engine is licensed via Hardkey and LPR configuration. The engine works with the plates from: Brazil, Argentina and Paraguay.

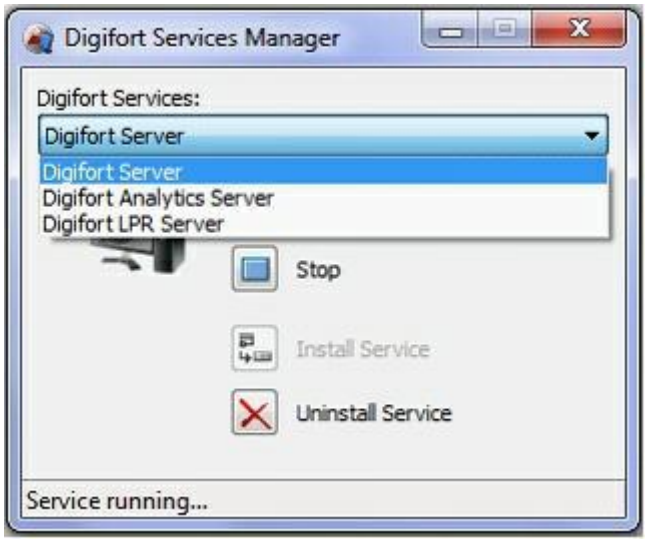
The **Carmen** engine is licensed via Hardkey which licenses a Core of the processor. This way the engine will process as many LPR as possible according to the Core processing capacity.



14.2.1 How to license the LPR Server

Once you have created the LPR server, you have to license it. As an example, we’ll use the Carmen license to begin with.
First of all, for Digifort to recognize the Hardkey in the computer, you must stop all server activity as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



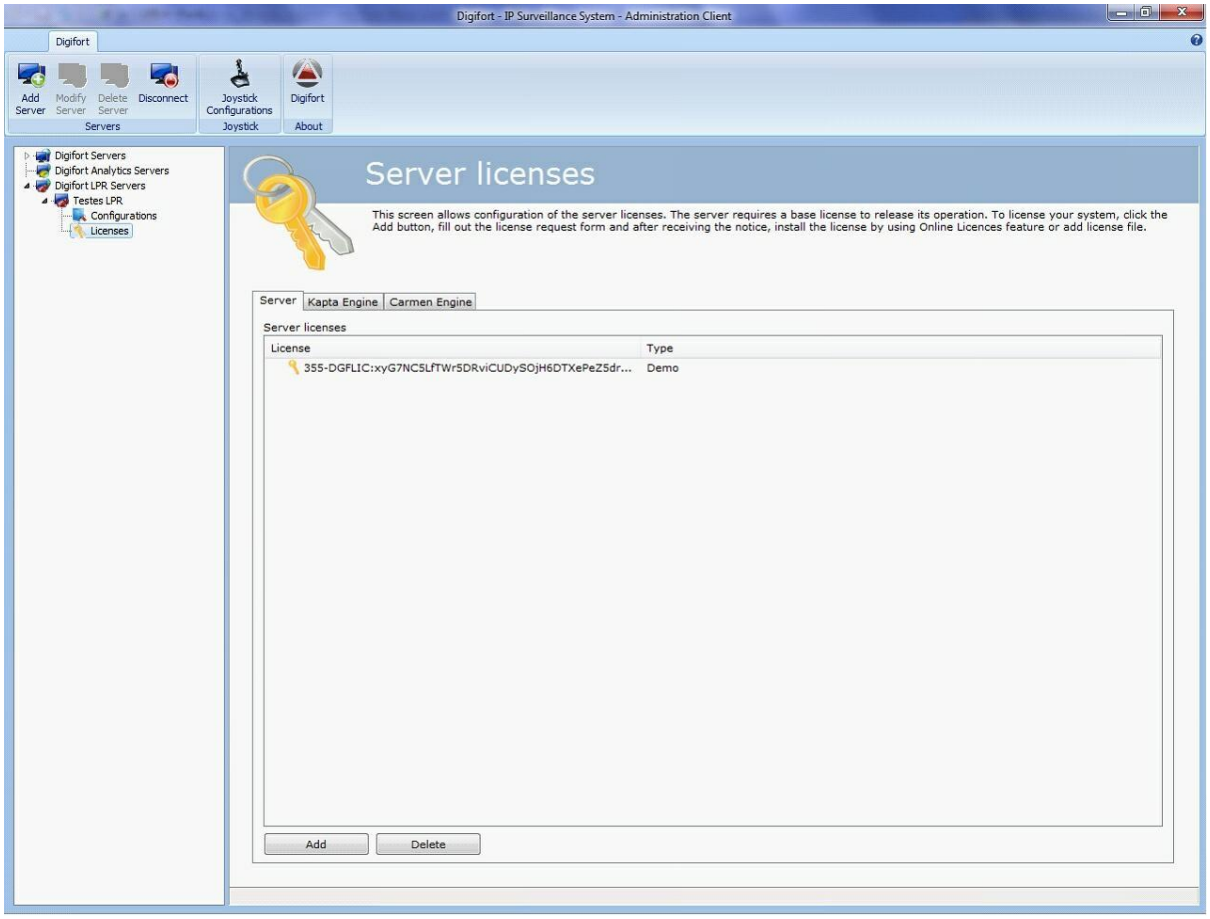
Note that the 6.4 version now includes three services:

- Digifort Server
- Digifort Analytics Server
- Digifort LPR Server

The Digifort Server and Digifort LPR Servers must be stopped. Now that the services have been stopped, you can connect the Hardkey to the computer and only then start the services again.

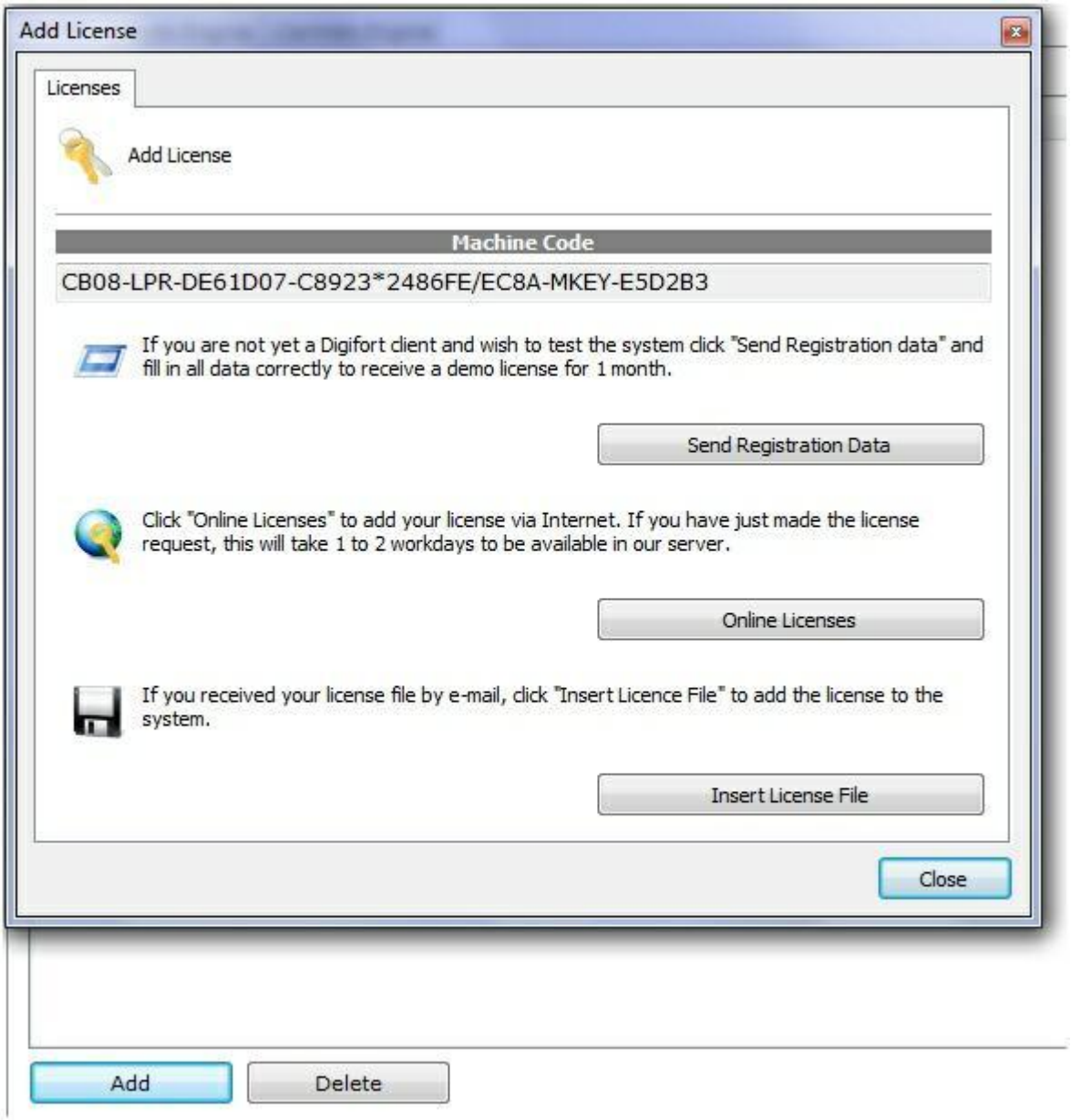
Now you can log into your LPR server and click on the “Licenses” option as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



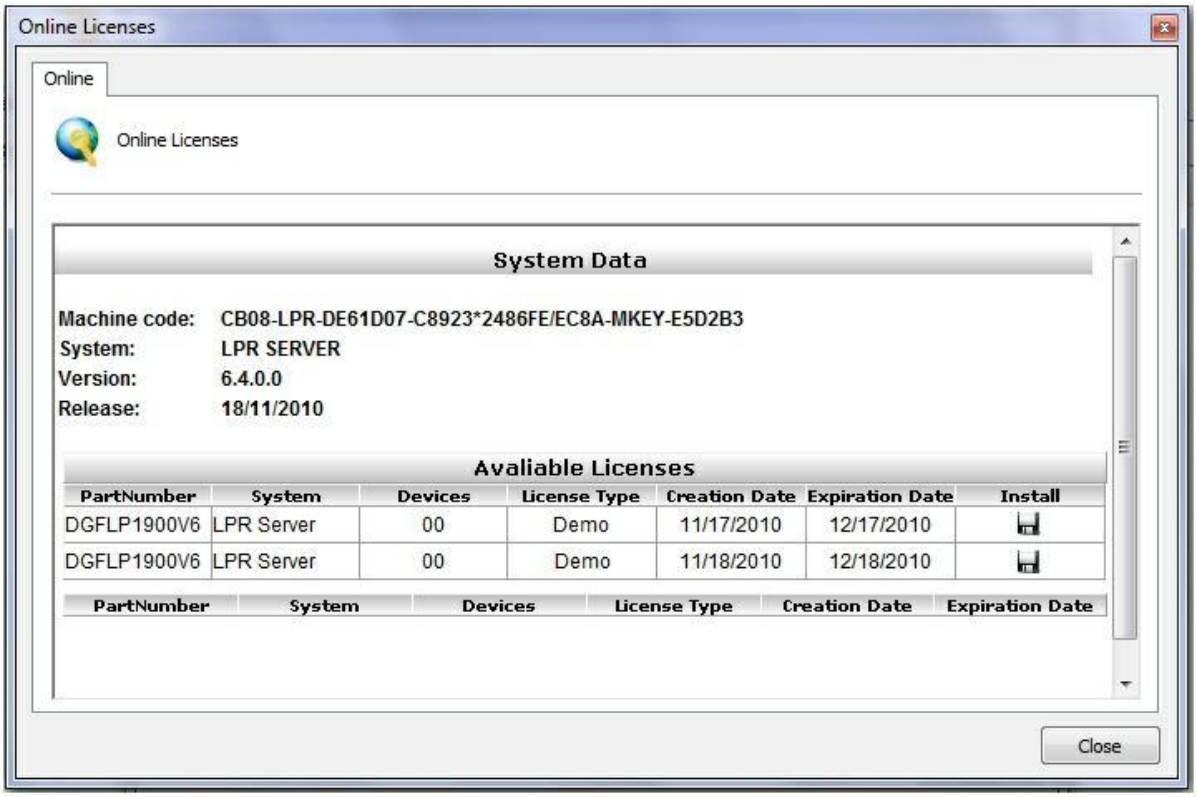
The base for the LPR to function will be installed in that Server tab.
The license is carried out on the Internet with the client information and a protocol number received by the client.
To install the base license, click on “Add” and the following screen will show up:

© 2002 - 2011 by Optiview USA all rights


Add License
Licenses
Add License
Machine Code
CB08-LPR-DE61D07-C8923*2486FE/EC8A-MKEY-E5D2B3
If you are not yet a Digifort client and wish to test the system click "Send Registration data" and fill in all data correctly to receive a demo license for 1 month.
Send Registration Data
Click "Online Licenses" to add your license via Internet. If you have just made the license request, this will take 1 to 2 workdays to be available in our server.
Online Licenses
If you received your license file by e-mail, click "Insert Licence File" to add the license to the system.
Insert License File
Close
Add
Delete

The licensing process is the same as for Digifort.
On the online license screen the description should be "LPR Server" as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



Once a license has been added it becomes available as shown in the picture below:


Server licenses
This screen allows configuration of the server licenses. The server requires a base license to release its operation. To license your system, click the Add button, fill out the license request form and after receiving the notice, install the license by using Online Licences feature or add license file.
Server
Kapta Engine
Carmen Engine
Server licenses
License
Type
355-DGFLIC:xyG7NC5LfTWr5DRviCUDySOjH6DTXePeZ5dr...
Demo

Now, let's configure the Engines.

14.2.1.1 How to license the Carmen engine

All the **Carmen** engine needs is that the Hardkey be plugged in and all the licenses are automatically recognized, as shown in the following picture:

© 2002 - 2011 by Optiview USA all rights



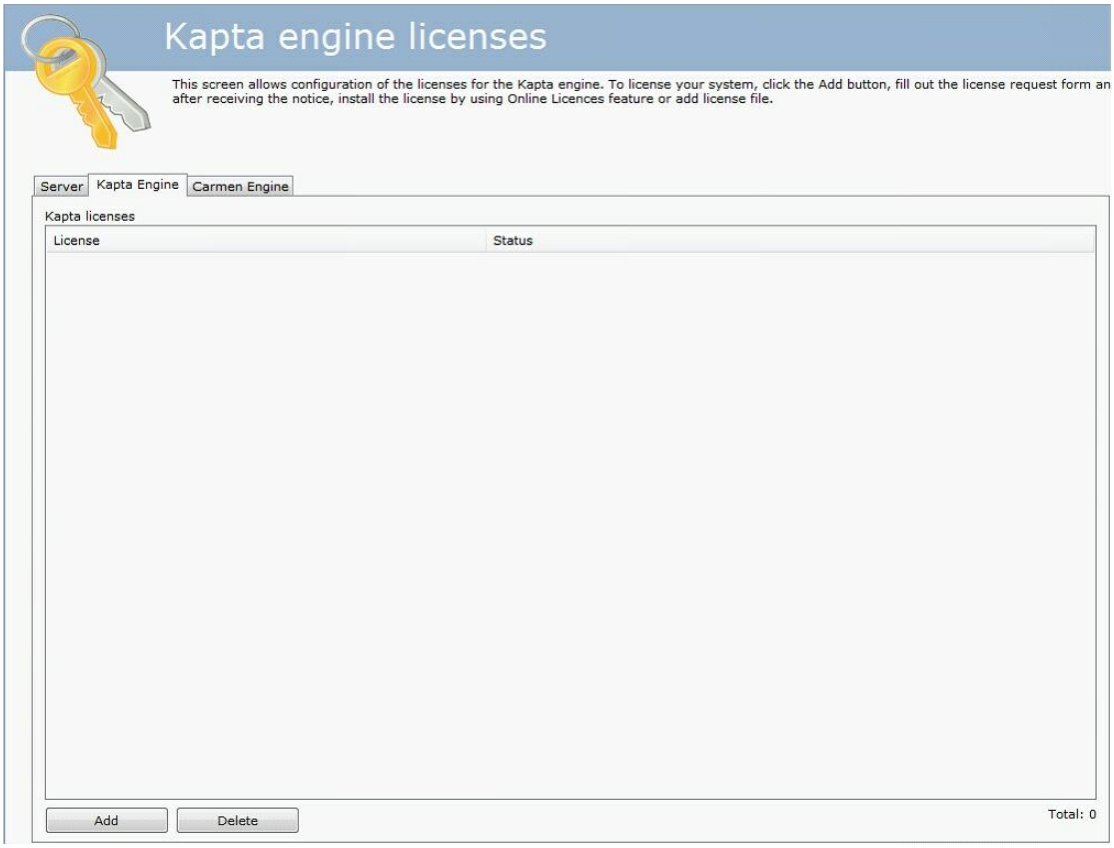
Pronto agora seu LPR com o **Engine Carmen** já está licenciado.

14.2.1.2 How to license the Kapta engine

The licensing procedure for this engine is slightly different. First, connect the Hardkey to the computer and carry out the same process to stop and start the Digifort service.

Your screen should look something like this:

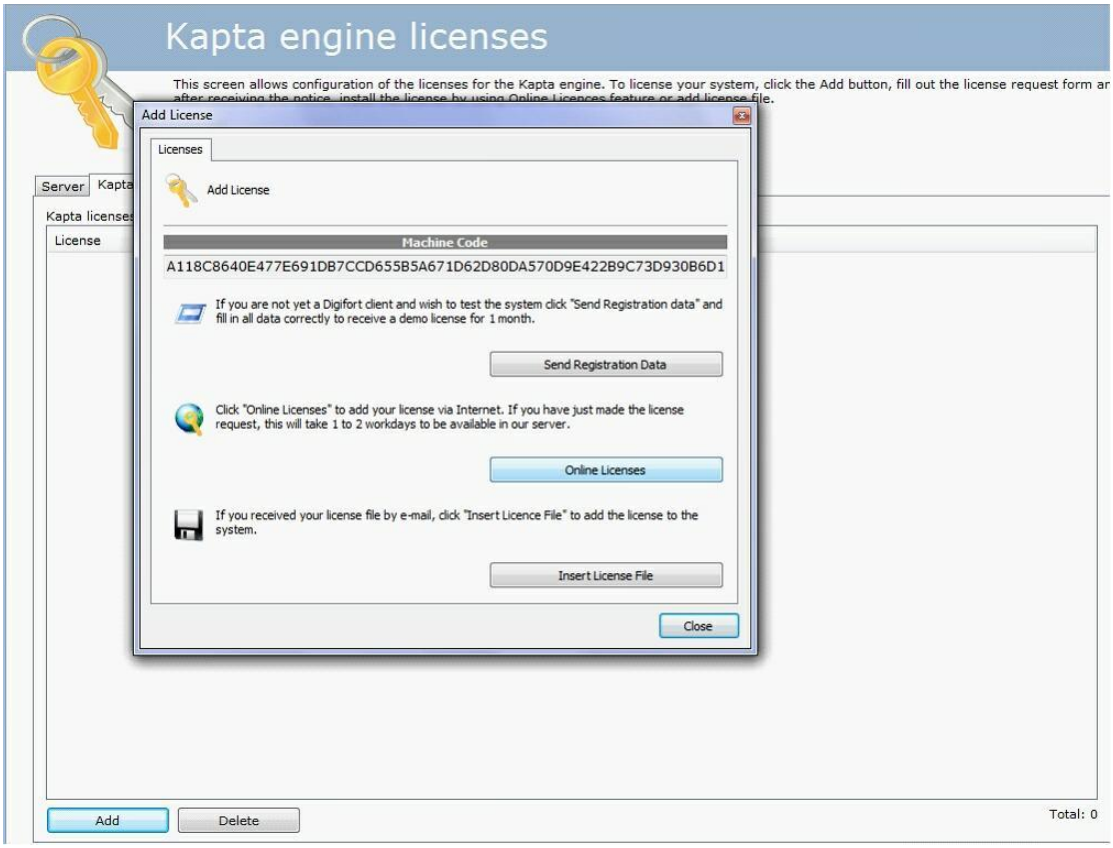
© 2002 - 2011 by Optiview USA all rights


Kapta engine licenses
This screen allows configuration of the licenses for the Kapta engine. To license your system, click the Add button, fill out the license request form an
after receiving the notice, install the license by using Online Licences feature or add license file.
Server
Kapta Engine
Carmen Engine
Kapta licenses
License
Status
Add
Delete
Total: 0

Click on Add to install the license as the Kapta engine generates a counter-password on the Hardkey so that you can install the licenses via the web.

After clicking on Add the following screen will open up:

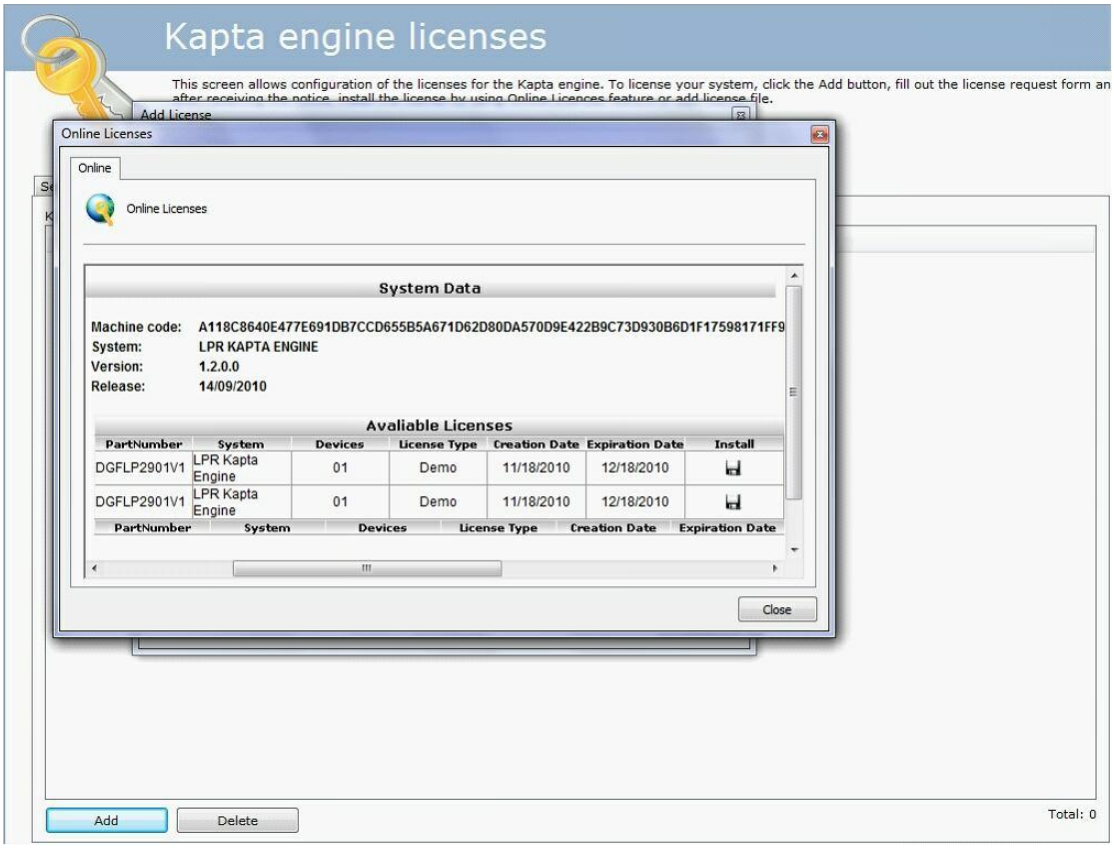
© 2002 - 2011 by Optiview USA all rights


Kapta engine licenses
This screen allows configuration of the licenses for the Kapta engine. To license your system, click the Add button, fill out the license request form ar
Server
Kapta
Kapta licenses
License
Add
Delete
Total: 0
Add License
Licenses
Add License
Machine Code
A118C8640E477E691DB7CCD655B5A671D62D80DA570D9E422B9C73D930B6D1
If you are not yet a Digifort client and wish to test the system click "Send Registration data" and fill in all data correctly to receive a demo license for 1 month.
Send Registration Data
Click "Online Licenses" to add your license via Internet. If you have just made the license request, this will take 1 to 2 workdays to be available in our server.
Online Licenses
If you received your license file by e-mail, click "Insert Licence File" to add the license to the system.
Insert License File
Close

Click on Online Licences so that you can see your licenses.

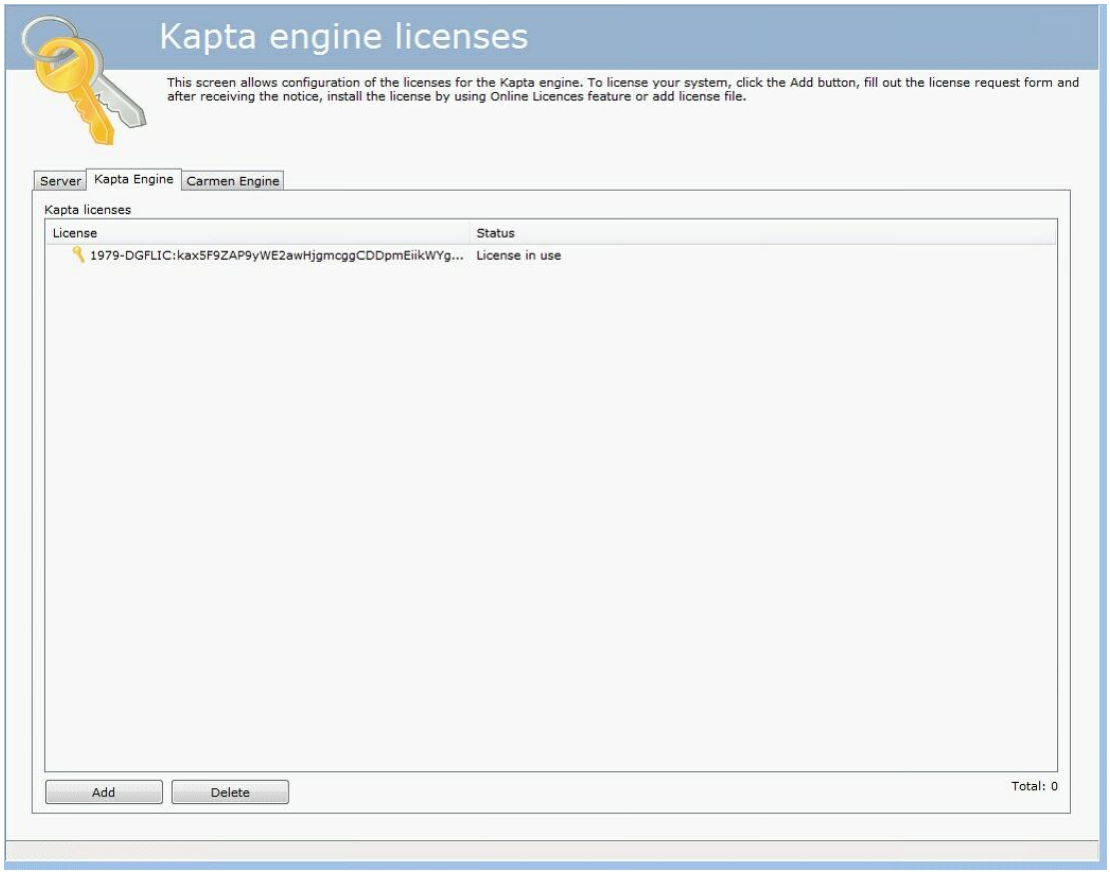
As the picture below shows, now you can install your Kapta engine licenses.

© 2002 - 2011 by Optiview USA all rights


Kapta engine licenses
This screen allows configuration of the licenses for the Kapta engine. To license your system, click the Add button, fill out the license request form an
Add License
Online Licenses
Online
Online Licenses
System Data
Machine code: A118C8640E477E691DB7CCD655B5A671D62D80DA570D9E422B9C73D930B6D1F17598171FF9
System: LPR KAPTA ENGINE
Version: 1.2.0.0
Release: 14/09/2010
Avaliable Licenses
PartNumber System Devices License Type Creation Date Expiration Date Install
DGFLP2901V1 LPR Kapta Engine 01 Demo 11/18/2010 12/18/2010
DGFLP2901V1 LPR Kapta Engine 01 Demo 11/18/2010 12/18/2010
PartNumber System Devices License Type Creation Date Expiration Date
Close
Add
Delete
Total: 0

Now the available licenses have been installed, they will show in the Kapta engine's start screen:

© 2002 - 2011 by Optiview USA all rights


Kapta engine licenses
This screen allows configuration of the licenses for the Kapta engine. To license your system, click the Add button, fill out the license request form and after receiving the notice, install the license by using Online Licences feature or add license file.
Server
Kapta Engine
Carmen Engine
Kapta licenses
License
Status
1979-DGFLIC:kax5F9ZAP9yWE2awHjgmcggCDDpmEiikWYg...
License in use
Add
Delete
Total: 0

Your Kapta engine is now licensed.

14.3 How to configure the License Plate recognition

To configure the plate recognition with the Carmen engine, you must first login to the Digifort server and, in **License Plate Recognition** choose **Configurations** as shown in the following picture:

© 2002 - 2011 by Optiview USA all rights



Click on **Add** and the following screen will show up:

© 2002 - 2011 by Optiview USA all rights


LPR configurations register
Use this register to register the LPR Configurations. The LPR Configuration is the core of the license plate recognition system, it will process the images from camera, extract and register found license plates and trigger alarms. On surveillance client you can add an LPR configuration on screen for live monitoring of the process.
LPR Configuration registration
General
Configurations
Rights
Name
Description
Camera
Perfil de mídia
Processing network
LPR Engine
Kapta
Carmen
Activate
OK
Cancel
Add
Modify
Delete

This screen has the following functionalities:

- **Name**: Name of the LPR chosen, for example: Digifort 1

- **Description**: Description of the analytics register, for example: License Plate Recognition on avenue 1.

- **Camera**: All the cameras registered in the Digifort server will be available in this selection box. To learn how to register cameras, refer to the chapter How to add a camera.
- **Media profile**: Select the media profile you want to use for the analysis. The analytics always analyses images with a resolution of 320x240 or 352x240, so it is recommended that these are the camera's minimum values.

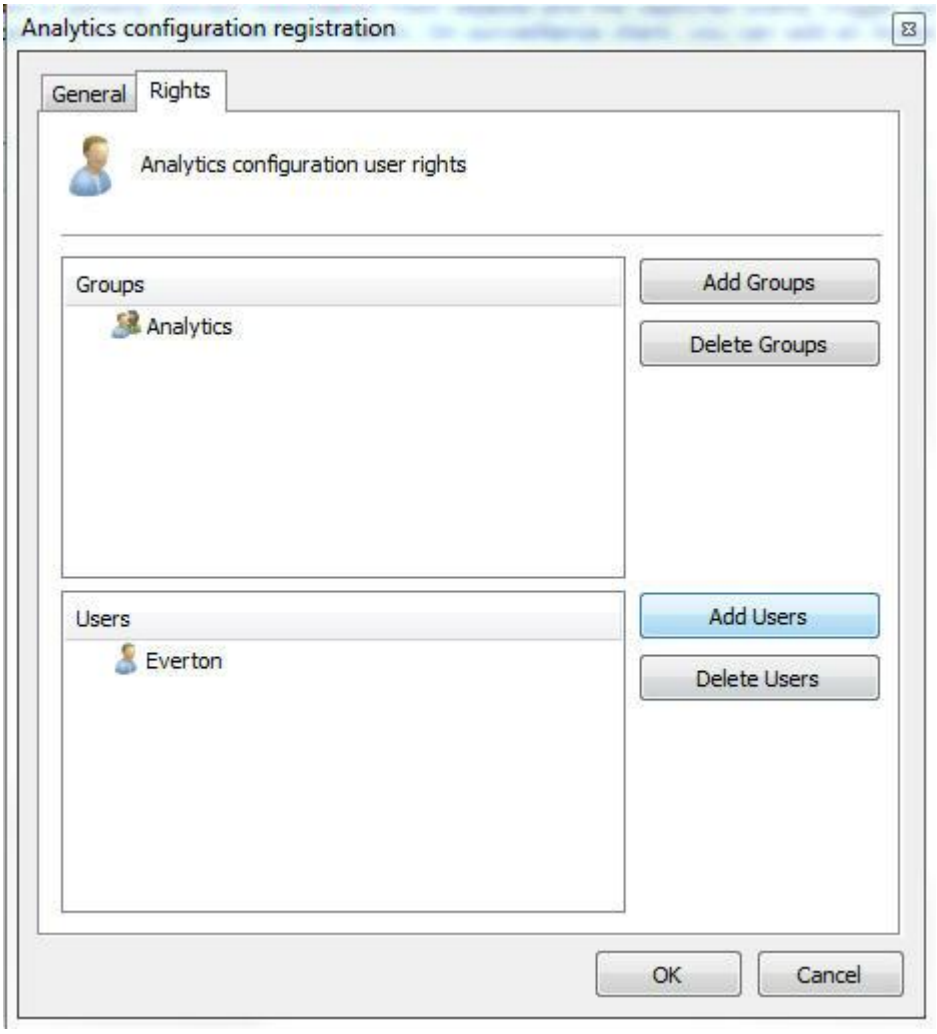
- **Processing Network**: All the "**processing networks**" (LPR servers) active on the network will be available in this field. Choose a network to process that configuration.

- **LPR Engine:** Choose the engine that will be analyzing the images. Digifort has two engines that process the images: Kapta and Carmen. Choose the engine obtained for the configurations.

- **Activate**: Activates or deactivates the analytics configuration.

In the configurations screen it is still possible to configure which users will be able to see this configuration. See the picture below:

© 2002 - 2011 by Optiview USA all rights

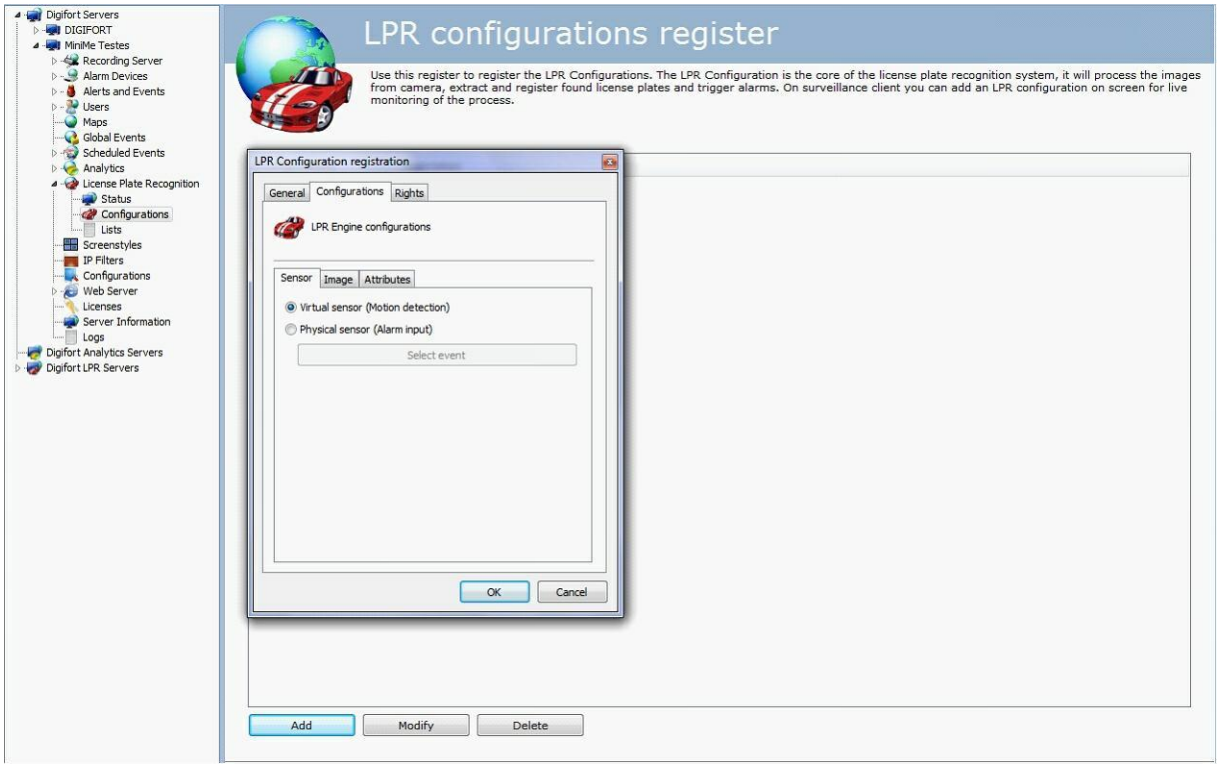


To learn about users and user groups refer to the chapter User Management .

14.3.1 Configuring the Carmen Engine

After configuring the **General** options, click on the **Configurations** tab.

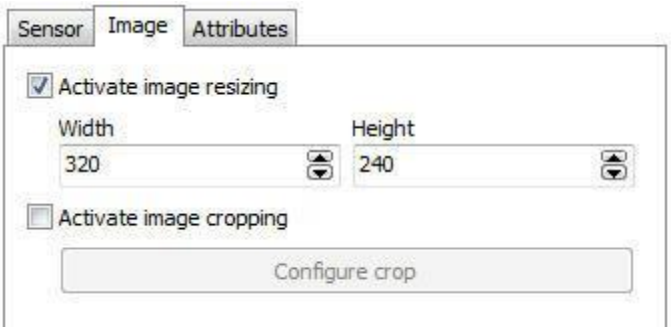
© 2002 - 2011 by Optiview USA all rights



Three configurations have to be made in this tab:

- **Sensor**: The sensor that will trigger the camera so that it can capture the license plate. It can be triggered by a **Physical Sensor**, or an infrared barrier, or a **Virtual Sensor** that will trigger the LPR on detecting movement.

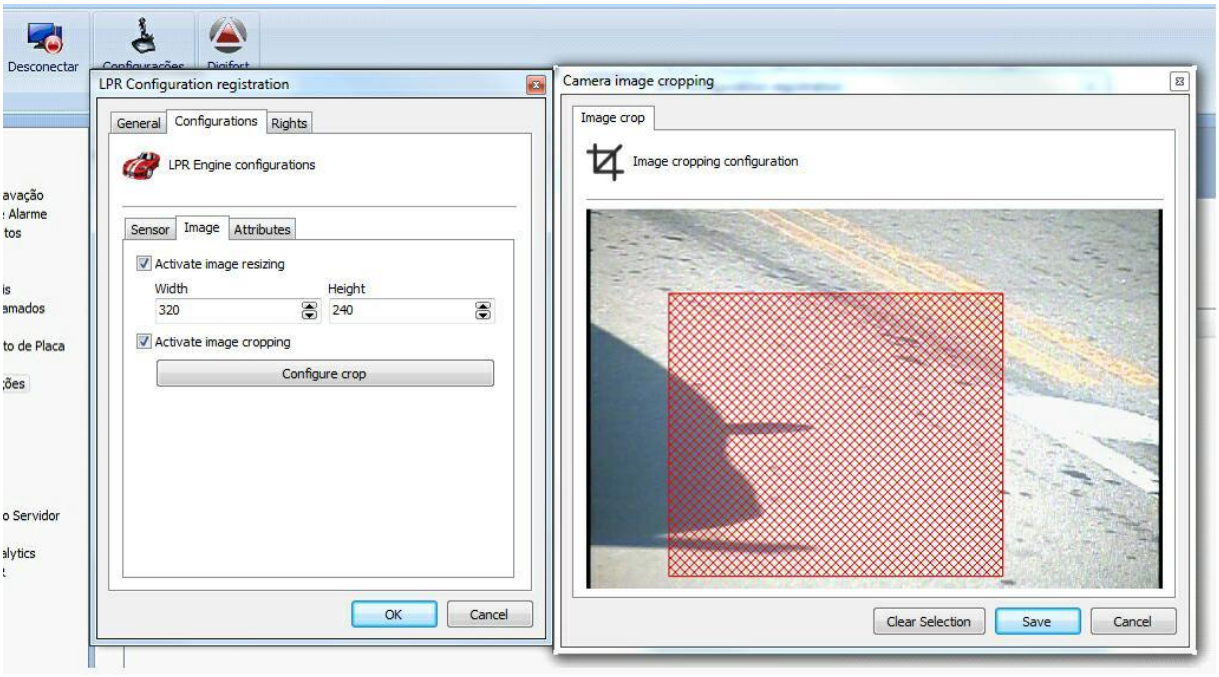
- **Image**: The following options are available in the Image tab:



We now have to:

  - **Activate image resizing:** This option changes the size of the photo captured by the camera so that there is less processing.
  - **Activate image cropping:** This option selects a specific area where the engine will look for license plates to be captured. This option is useful when there is a mega pixel camera that can cover several lanes with vehicles. For example:

© 2002 - 2011 by Optiview USA all rights



· **Features**: Below are the options available:



· **Activate character mask**: This option allows greater control of what the software will be identifying on a number plate. The 0 character only identifies numbers, **A** only identifies letters, and **X** identifies letters and numbers. If, for example, the license plate pattern you want to capture is EGV - 1234 then the best filter to configure is AAA000.

· **License plate character count**: This option is used to configure a **Minimum** and **Maximum** number of characters to be identified by the recognition process. This option is useful because the number of

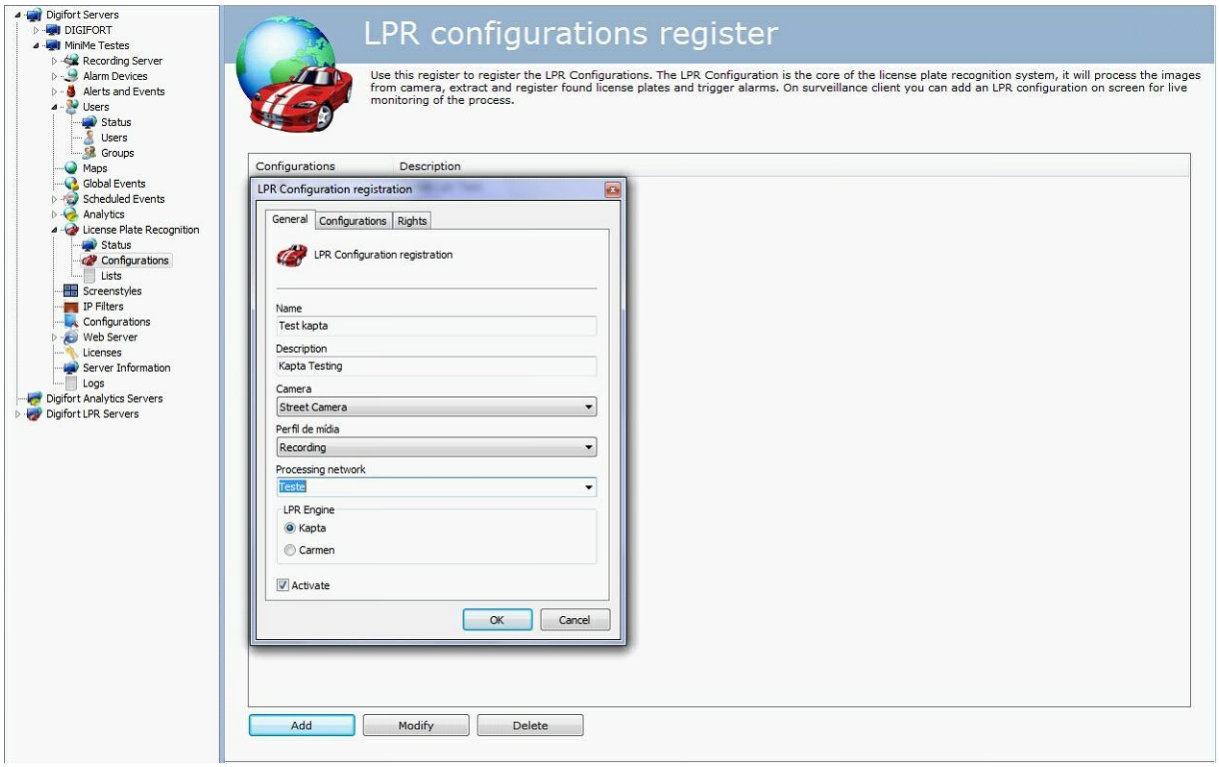
© 2002 - 2011 by Optiview USA all rights

characters varies from country to country.

14.3.2 Configuring the Kapta Engine

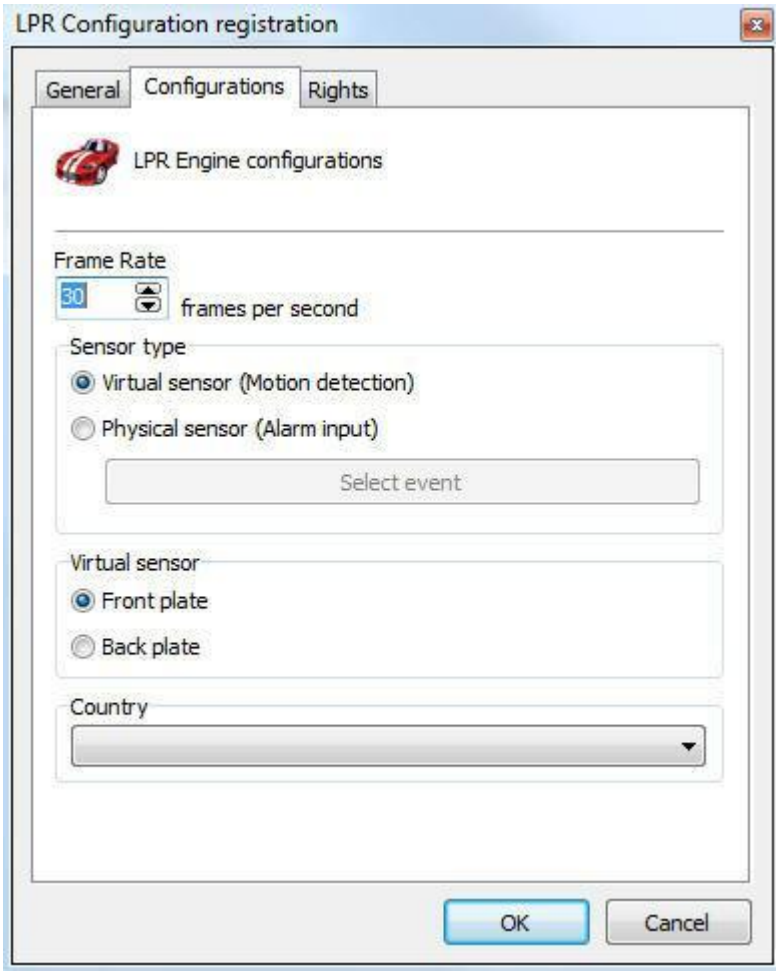
After configuring the **General** options, click on the **Configurations** tab.

Only a few configurations are different from the Carmen engine to the Kapta engine. The first part is exactly the same, the only difference being that you have to select the Kapta Engine as shown below:



The following options are available in the **Configurations** tab:

© 2002 - 2011 by Optiview USA all rights



- **Frame Rate**: The number of frames sent to the engine to be analyzed.

- **Sensor**: The sensor that will trigger the camera so that it can capture the license plate. It can be triggered by a sensor.

- **Virtual Sensor**: The **Front Plate** option must be selected if the plate recognition is to be made from the front of the car. The **Back Plate** option must be selected if the plate recognition is to be made from the back side of the car.

- **Physical Sensor:** This option will trigger the plate recognition based on a command sent by a Digifort event. Recognition may be triggered by the commbox with an Infrared barrier, for example, or by a connected magnetic sensor, or even a sensor connected to a camera's I/O.

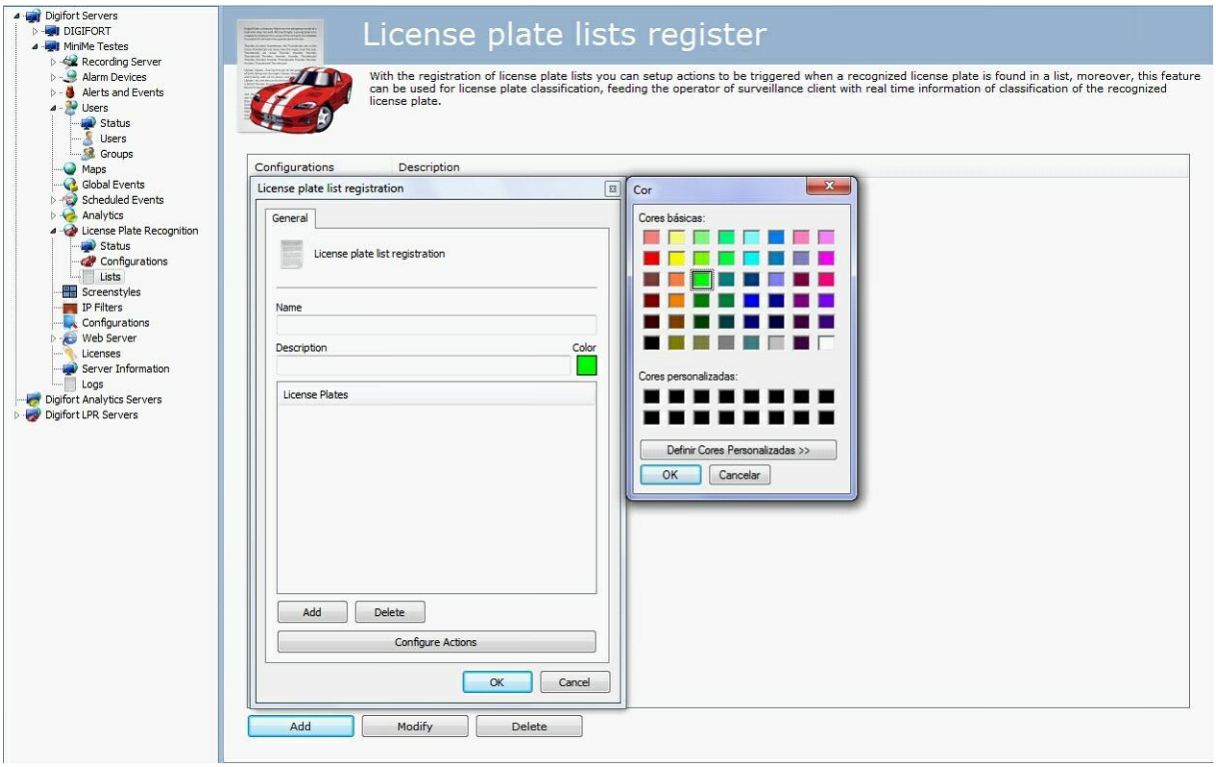
- **Country**: Select the country of the license plate for the engine to recognize.

© 2002 - 2011 by Optiview USA all rights

14.3.3 Configuring the LPR lists

As well as the Capture and Identification of vehicle license plates in Digifort, the LPR can also create a number of alerts when an already registered license is recognized. The configuration for such alerts is the same for both the Carmen and the Kapta Engines.

To create an option we have to enter the Lists option as shown in the following picture:



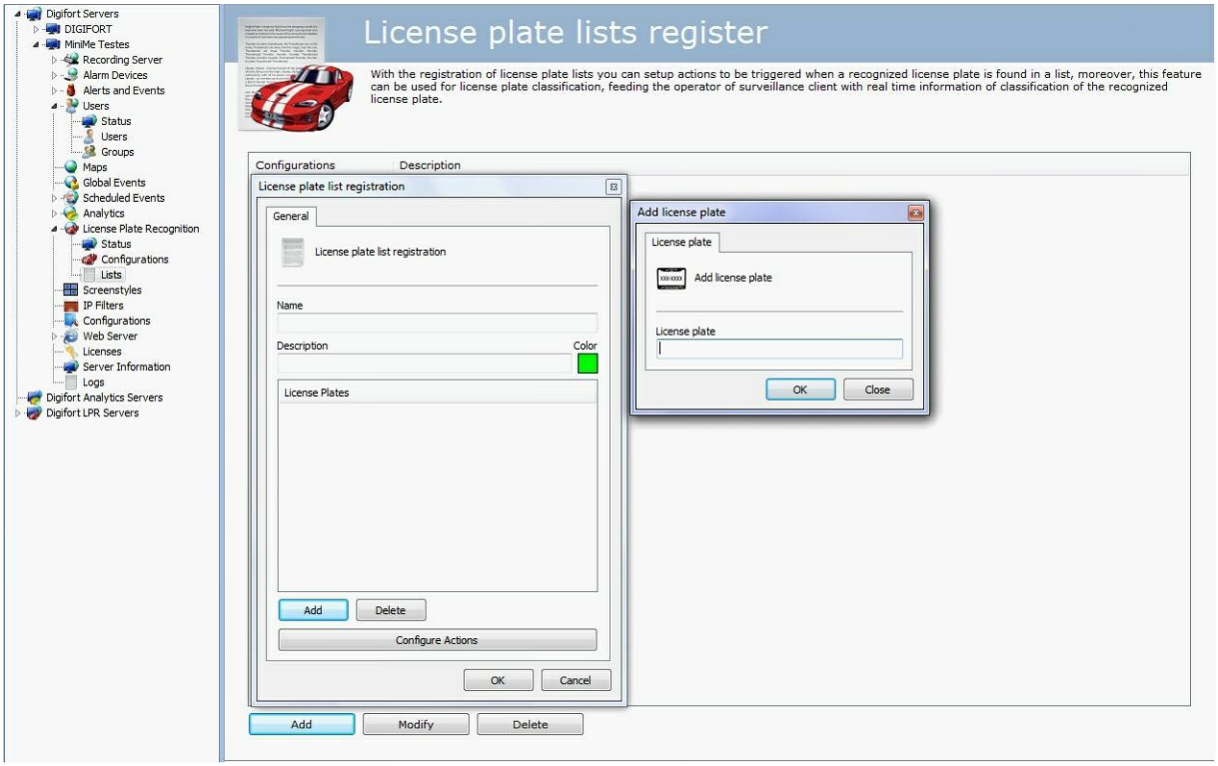
In this screen, click on Add. When you have clicked, the license plate registration screen will show up with the fields that have to be filled in:

- **Name**: Name given to the list. Example: Entrance List 1, Town List 2.
- **Description**: Description given to the list. Example: Stolen vehicles, authorized vehicles, etc.
- **Colour**: Colour associated to this list. This colour will be visible in the Surveillance Client when the list triggers an alert.
- **License Plates**: List of license that will trigger the alerts.
- **Configure actions**: In the alerts screen configure the actions chosen when the analytics triggers the events. To learn more about alert actions, refer to the chapter How to configure alarm actions .

After clicking on **"Add"** a new screen will show up where you can register any chosen license plates.

Click on Add to register the license plates in the list. The screen to register a license plate is similar to the one shown below:

© 2002 - 2011 by Optiview USA all rights



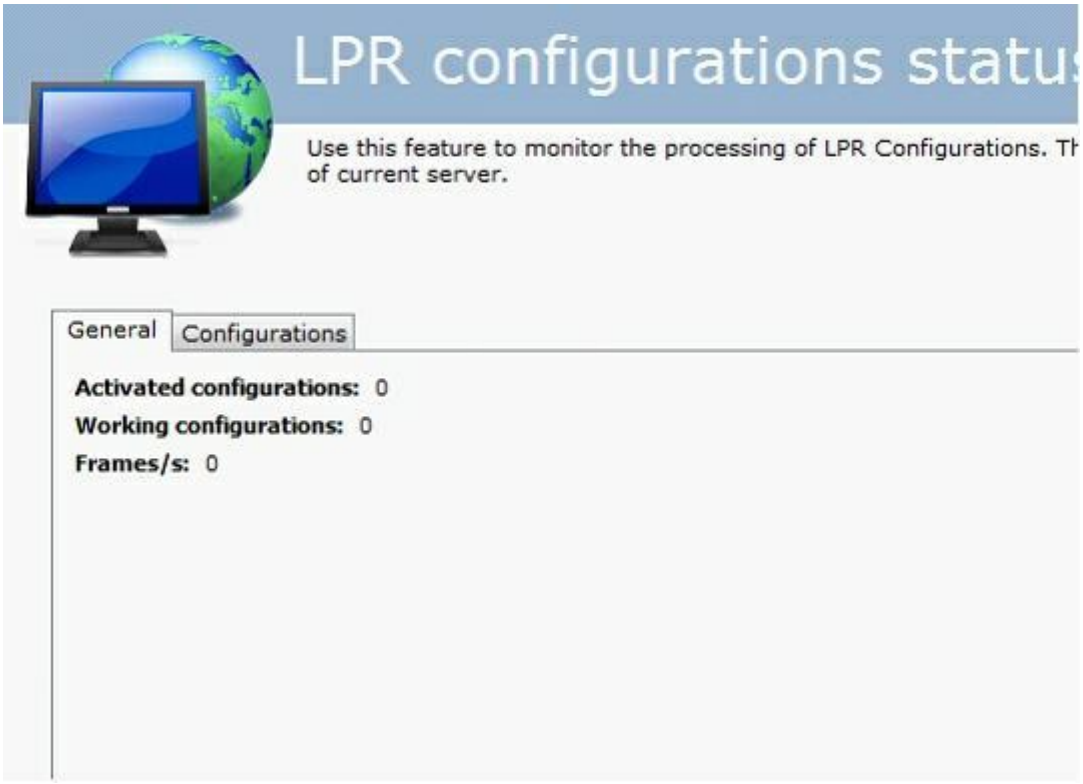
Once you have registered the license plates and selected the actions, the configuration is ready.

14.3.4 Verifying the LPR Status

The Status option will give you all the information on LPR configurations, such as: number of active LPR configurations, number of active LPR configurations, among other functions shown below.

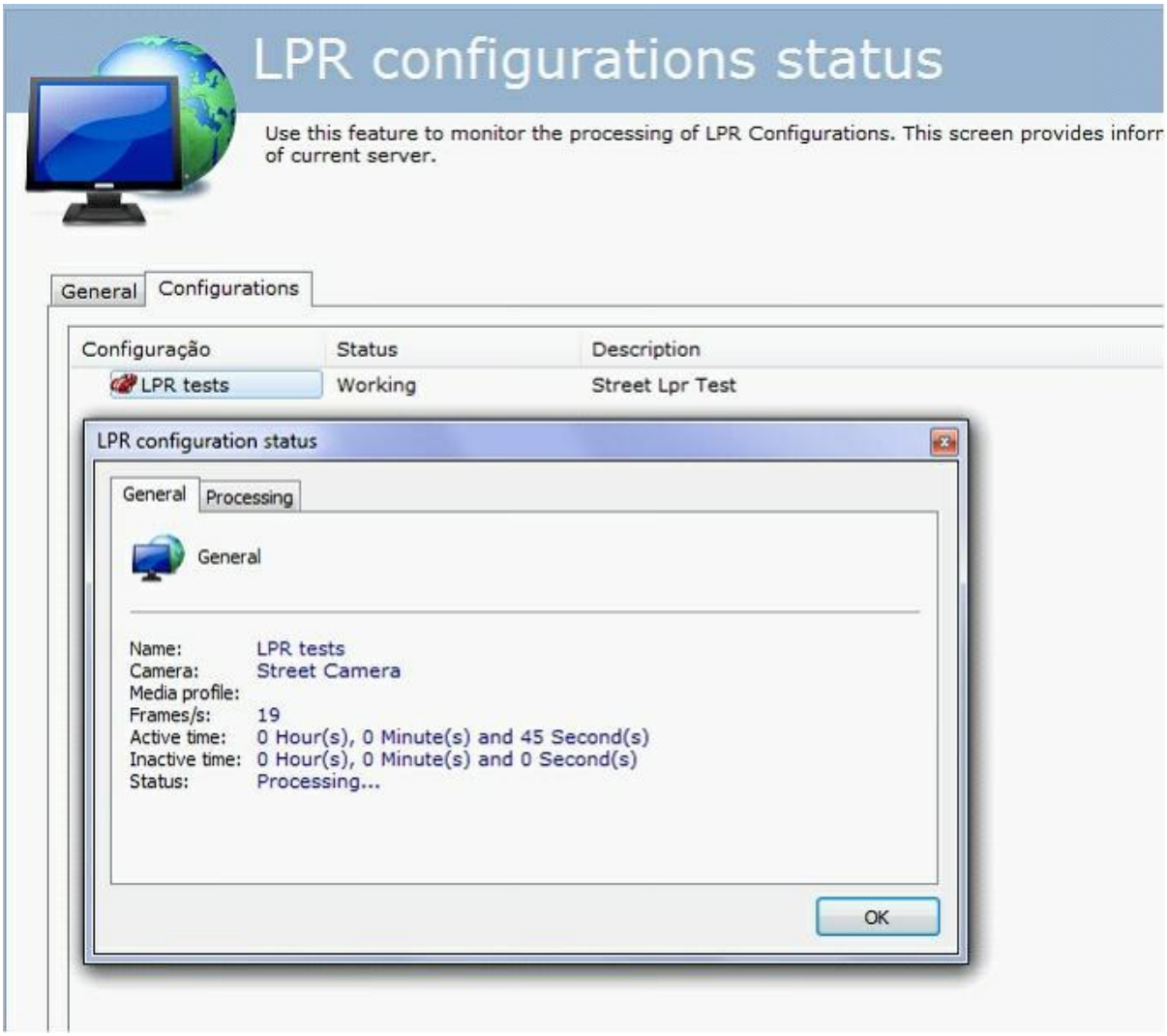
With the **Status** option you can check different information regarding the configurations made as shown in the following pictures:

© 2002 - 2011 by Optiview USA all rights



- **Active Configurations**: LPR configurations active at the time.
- **Working Configurations**: Working LPR configurations.
- **Frames**: Number of frames processed.

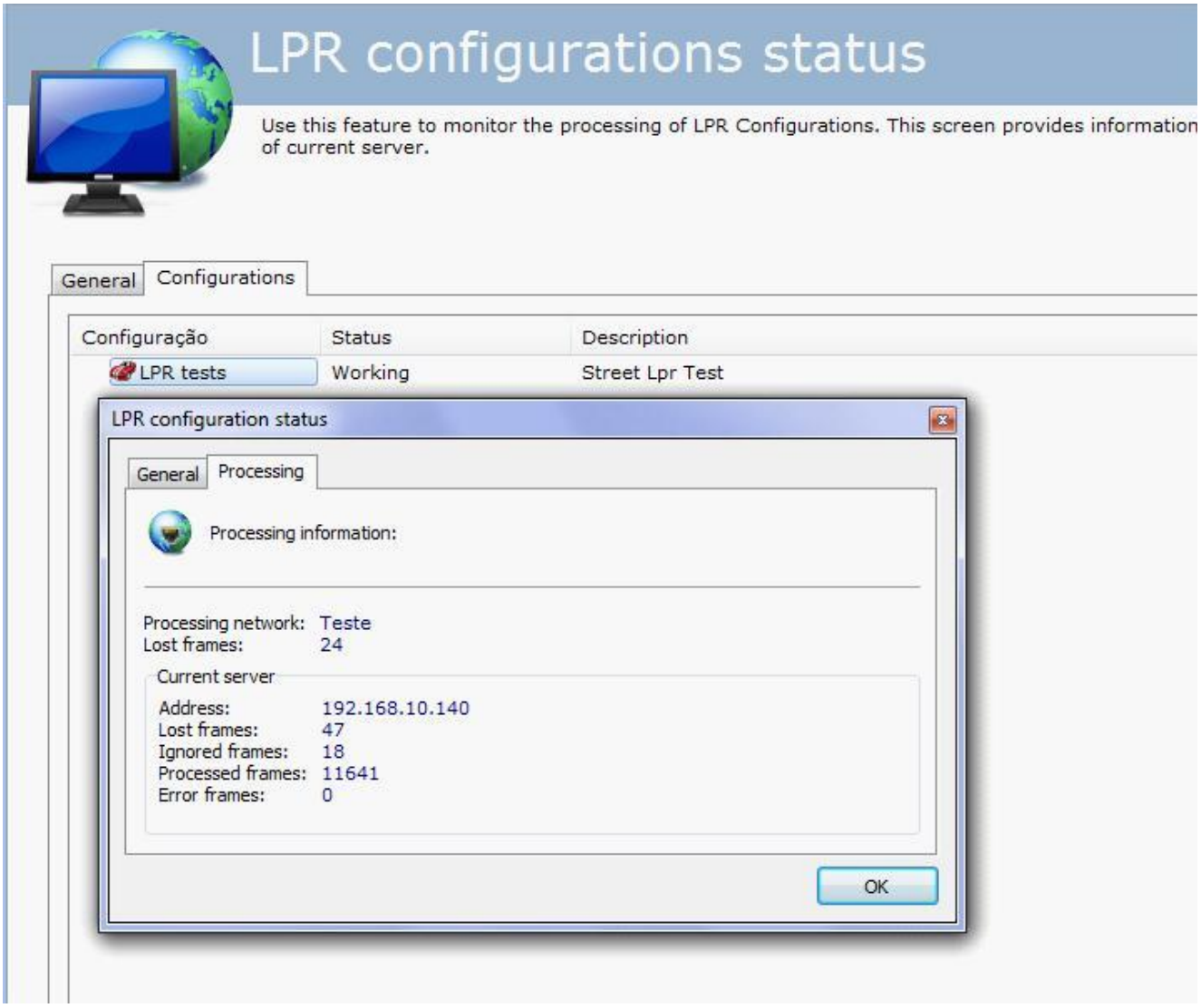
© 2002 - 2011 by Optiview USA all rights



In the **General** tab you'll have information such as:

- **Name**: Name of the active configuration
- **Camera**: Name of the camera being processed by the engine.
- **Media profile**: Media profile used for processing.
- **Frames**: Number of frames processed.
- **Active Time**: Time the configuration has been active up to that point.
- **Inactive Time**: Time the configuration has been inactive to that point.
- **Status**: Status of the active configuration.

© 2002 - 2011 by Optiview USA all rights



- **Processing Network:** Name of the processing network that is processing the current configuration.
- **Lost Frames:** Frames perdidos na análise no Servidor.

Current server:

- **Address**: Address where the configuration is being processed.
- **Ignored Frames**: Frames ignored by the server.
- **Processed Frames**: Total frames processed.
- **Error frames**: Frames that reached the server with errors.

© 2002 - 2011 by Optiview USA all rights

Chapter XV

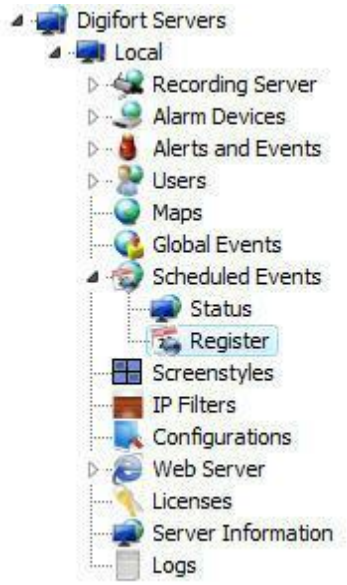
15 Sheduled Events

Sheduled events allow the user to create scheduled actions for executing some system function at specified dates and times.

This feature is very useful for automating and easing routine tasks such as turning on lights, opening doors and controlling the activation of any kind of equipment at the Sheduled time.

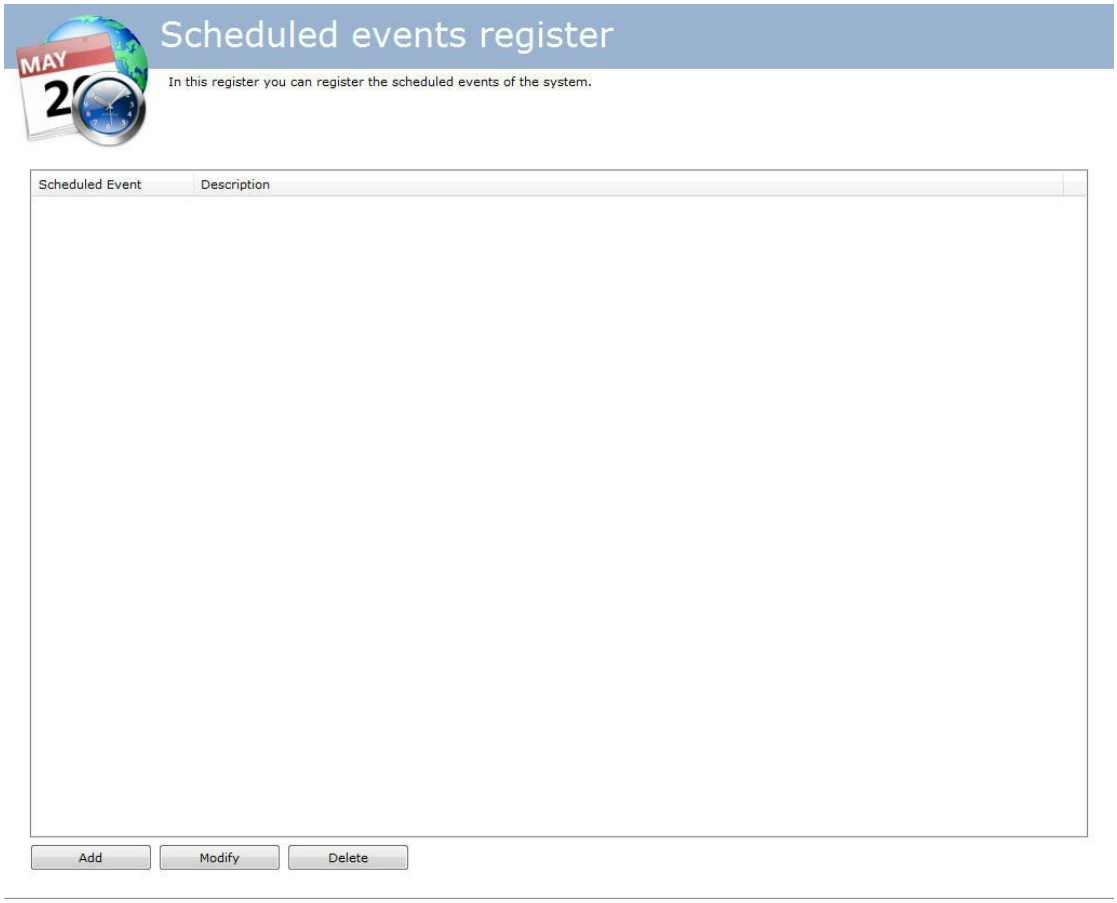
15.1 Registering Sheduled Event

To access this area, click on the Register tab in the Menu of Sheduled Events, as shown in Figure bellow:



Once this is done, the general system configuration screen will open up at the right, as shown in Figure bellow:

© 2002 - 2011 by Optiview USA all rights

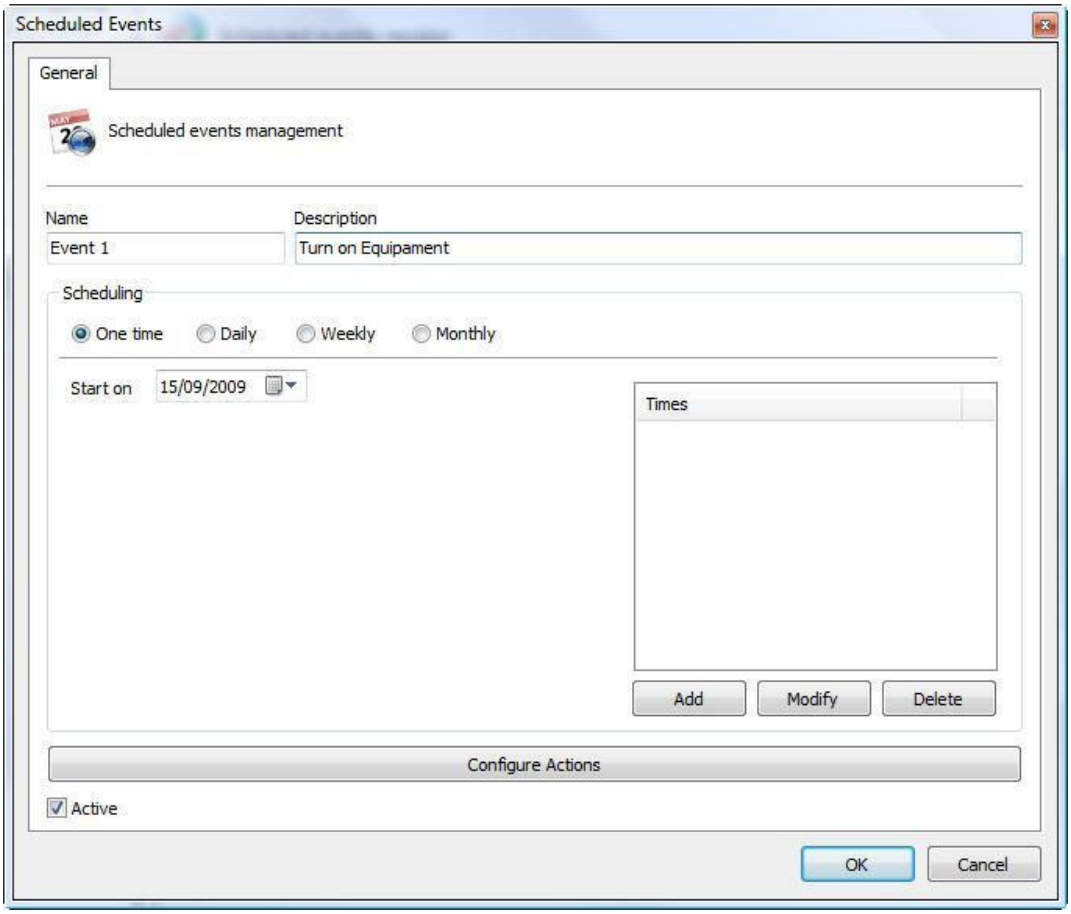


To add a Sheduled Event, click on **Add**. To modify or delete a Sheduled Event, select the desired camera and click on the corresponding button.

15.1.1 Adding Sheduled Event

After clicking on **Add**, the event registration screen will open up as shown in the figure below:

© 2002 - 2011 by Optiview USA all rights



This screen offers the following function:

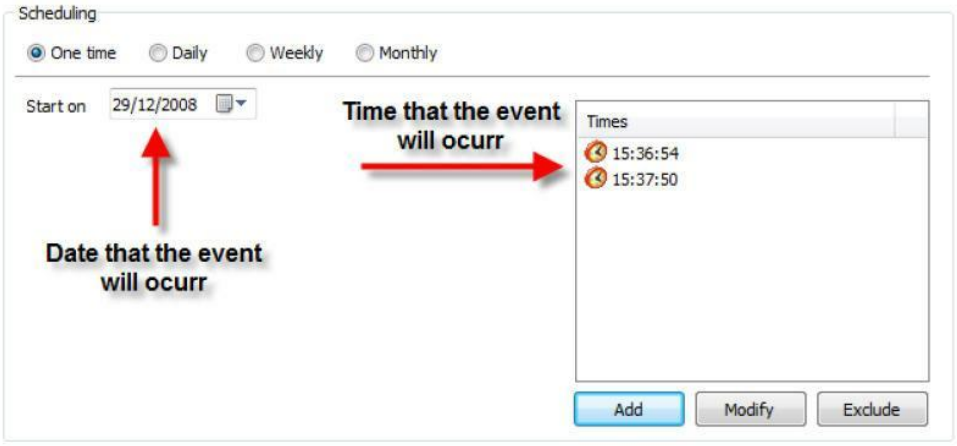
- **Name**: Enter the desired name for the event. This name will be the key for recognition in the system.
- **Description**: The desired description for the event to be registered.
- **Scheduling**: The type of scheduling to be made. The event can be activated only once, daily, weekly or monthly. The types of scheduling will be explained further on.
- **Times**: Screen in which one or more times of day can be added for the event to be activated.
- **Configure Actions**: Click on this button to configure the actions that Digifort will carry out when this event occurs. To learn how to configure the actions that this manual event will execute, see How to configure the alarm actions
- **Active**: Active or de-Active the event.

15.1.1.1 Types of Scheduling

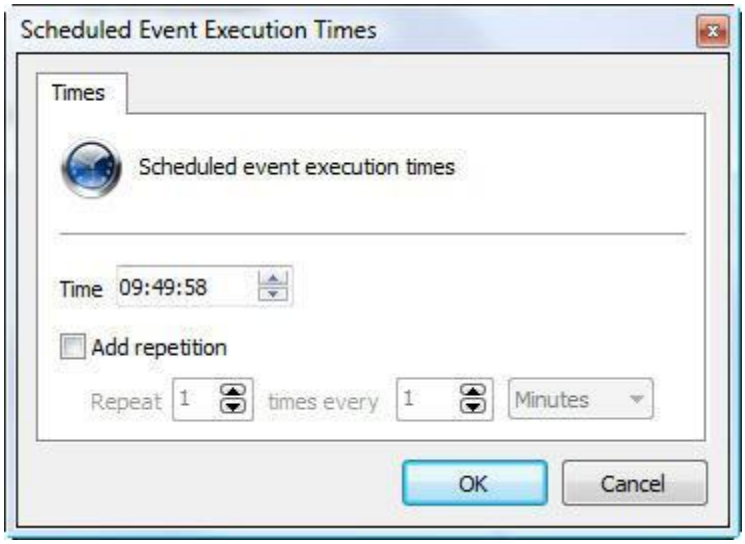
15.1.1.1.1 Only once

In this option, only the options for the date and time of the execution of the event will be configured as shown by the figure below:

© 2002 - 2011 by Optiview USA all rights



First, select the date on which the event shall occur, followed by clicking on Add in the times window and the following screen will be displayed:



In this window, select the desired time of day for execution of the event. If necessary, the repetition of the event every X minutes can be added.

The time of day will remain in the screen as shown by the Figure below:

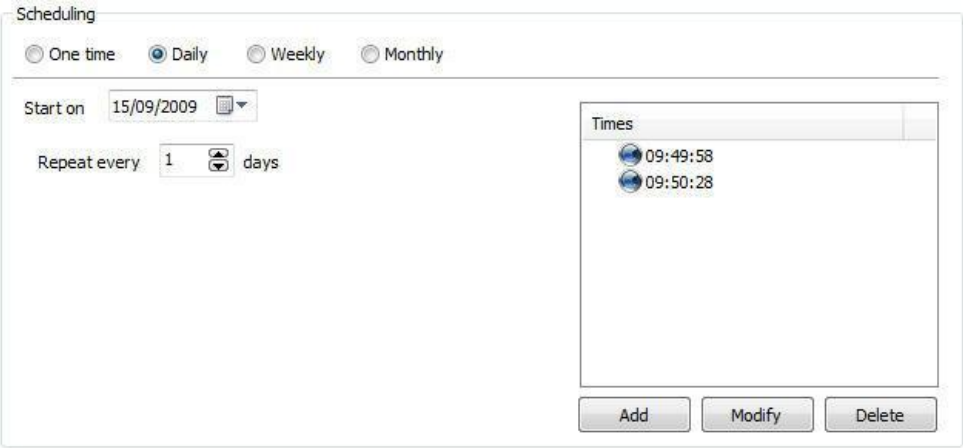
© 2002 - 2011 by Optiview USA all rights



NOTE: As many times of day can be added as necessary by simply repeating the process.

15.1.1.1.2 Daily

In this option, the same setting as before are presented with exection of the field shown in the figure below:



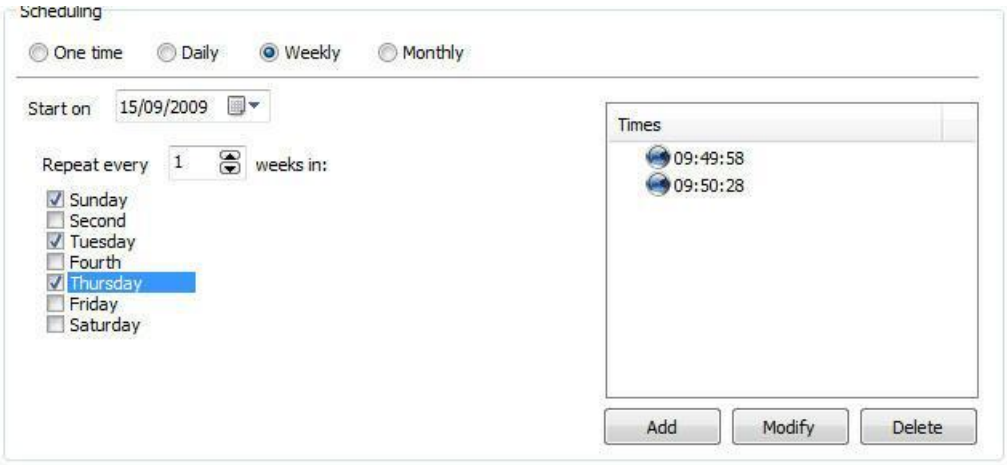
This field allow the event to occur every day (as the figure shows) or every other day, every third day, and so on, depending on the number configured.

15.1.1.1.3 Weekly

The Weekly scheduling allow the event to be repeated every X weeks, at the defined times and on the desired days of the week.

The options of weekly sceduling are shown in the figure below:

© 2002 - 2011 by Optiview USA all rights



This screen offers the following functions:

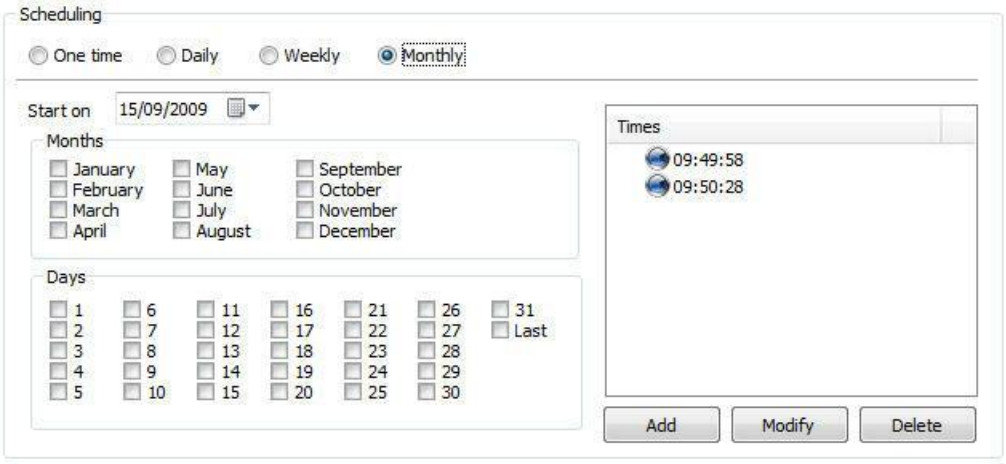
- **Start on**: Starting date of the event. In the case of weekly scheduling, the software will assume the current week as the beginning, that is, the following week will start on the next Sunday.
- **Repeat every X weeks on**: Repeat the event every X weeks (every other week, every three weeks, etc.) on the desired days. Just click on the days on which the event shall occur.
- **Times**: Add the times of day on which the event shall occur.
- **Configure Actions**: Click on this button to configure the actions that Digifort will carry out when this event occurs. To learn how to configure the actions that this manual event will execute, see How to configure the alarm actions

15.1.1.1.4 Monthly

In the monthly configuration it's possible to choose the desired months and days for the determined event to occur.

The months registration screen is shown in the figure below:

© 2002 - 2011 by Optiview USA all rights



This screen offers the following functions:

- **Start on**: Starting date of the event. Select the desired date for beginning of the events.
- **Months**: Select the desired months during which the events shall occur.
- **Days**: Select the desired days on which the events shall occur.
- **Times**: Add the times of day at which the events shall occur.
- **Configure Actions**: Click on this button to configure the actions that Digifort will carry out when this event occurs. To learn how to configure the actions that this manual event will execute, see How to configure the alarm actions

© 2002 - 2011 by Optiview USA all rights

Chapter XVI

16 Screenstyle Administration

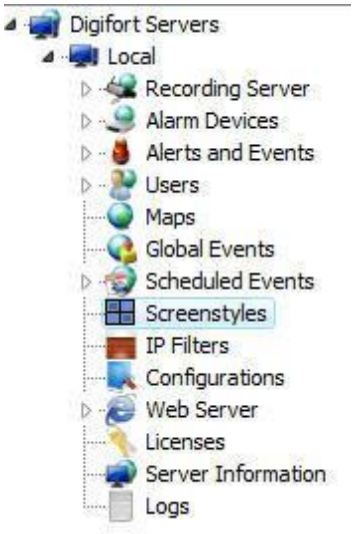
Screenstyles are groupings of cameras in a determined format and order that are used by the Surveillance Client to exhibit the cameras in the screen.

In addition to pre-defined screenstyles, Digifort Enterprise allows for the creation of new types of screenstyles, aimed at customization of the system according to the user's taste.

In the Administration Client, it's possible to administer the screenstyles, that is, their creation, modification or exclusion. To learn how to add cameras to the screenstyles, consult the manual of the Surveillance Client. Cliente de Monitoramento.

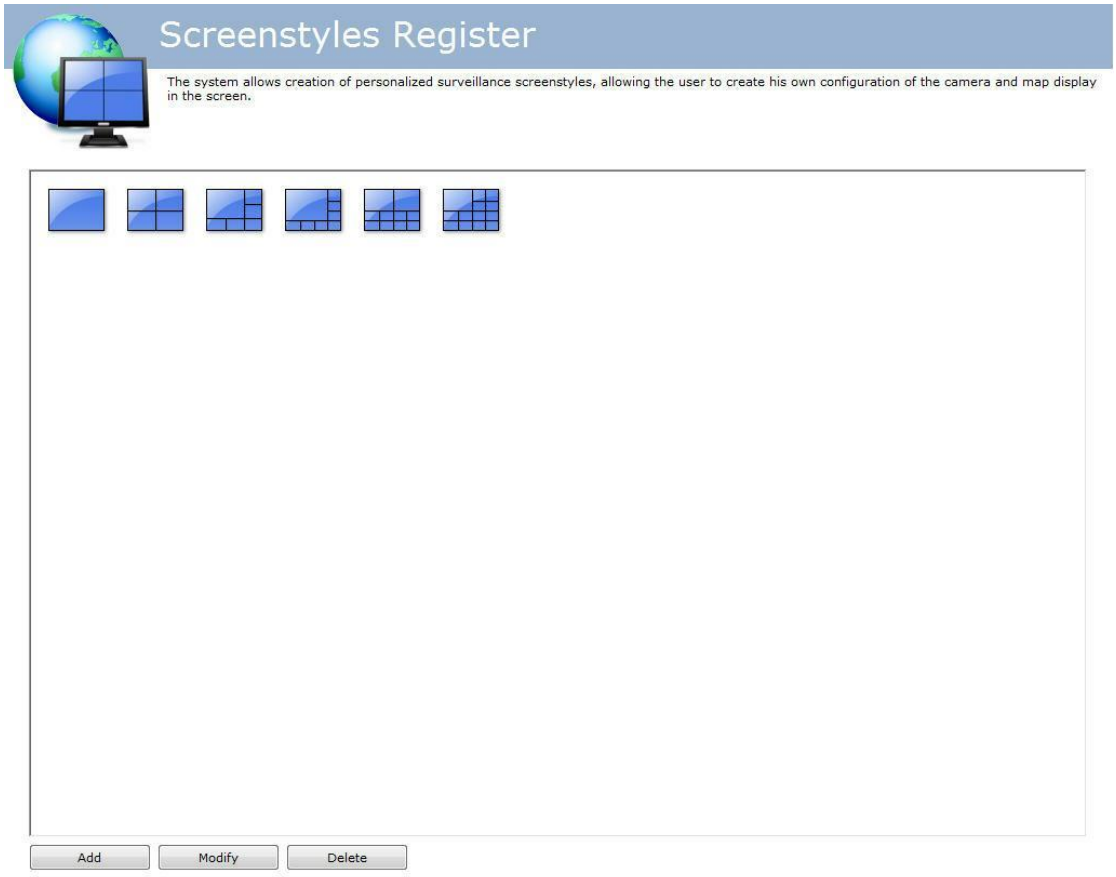
16.1 How to access the screenstyle administration

To access the screenstyle administration, locate the item Screenstyles in the Configurations Menu, as shown in the picture below:



Once this is done, the screenstyles register will be displayed at the right, as shown in the picture below:

© 2002 - 2011 by Digifort, all rights reserved

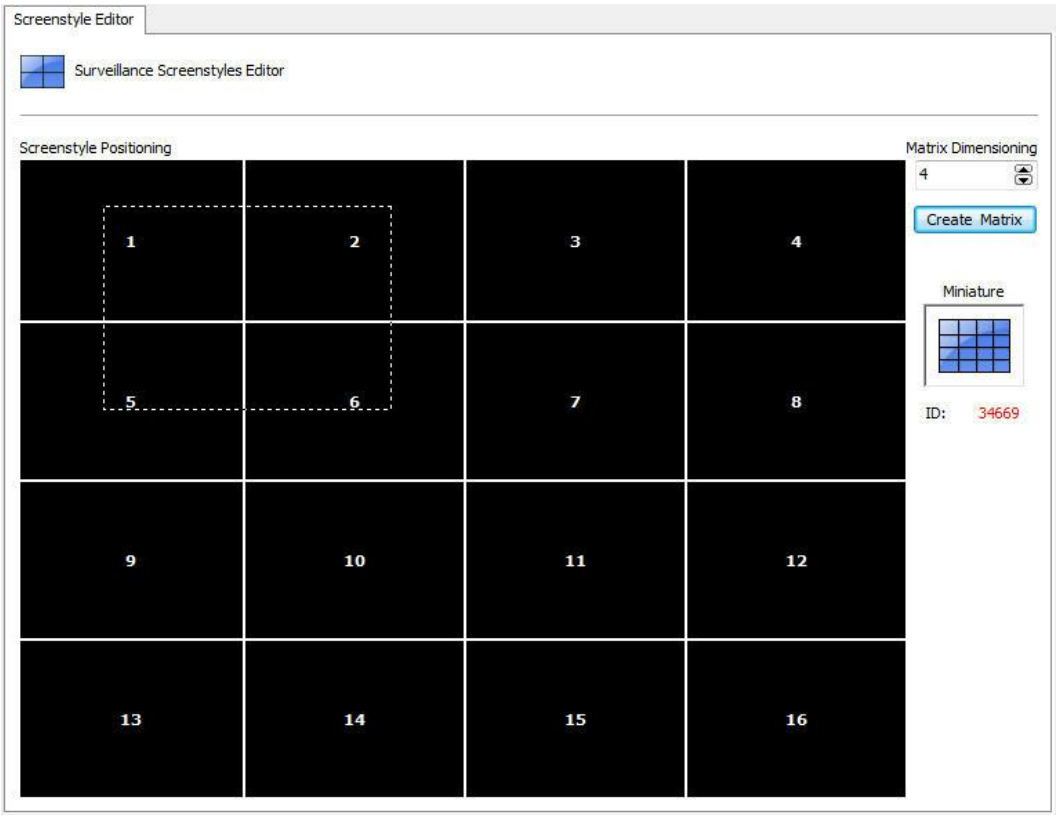

Screenstyles Register
The system allows creation of personalized surveillance screenstyles, allowing the user to create his own configuration of the camera and map display in the screen.
Add
Modify
Delete

Digifort Enterprise offers six pre-defined screenstyles that cannot be modified or excluded. To add a screenstyle, click on Add. To modify or exclude a screenstyle, select it and click on the corresponding button.

16.1.1 How to add a screenstyle

After clicking on **Add**, as explained in the previous topic, the following screen will be displayed:

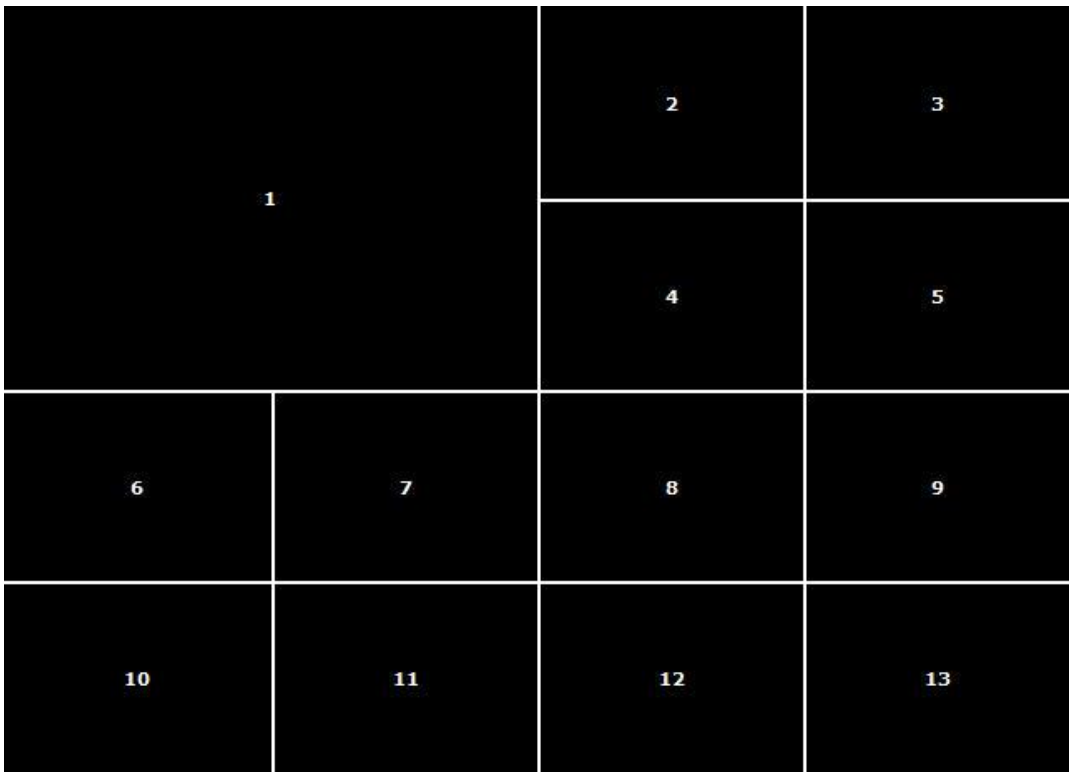
© 2002 - 2011 by Digifort, all rights reserved



In the picture above we created a 4x4 matrix, making it possible to add 16 cameras to the screen.

After creating the matrix, it's possible to join the quadrants, clicking on the left button of the mouse and dragging it, with the purpose of having a larger visualization area. In the example above, we are joining the quadrants 1, 2, 5 and 6, forming the screenstyle presented in the picture below:

© 2002 - 2011 by Digifort, all rights reserved



By joining these four quadrants we obtain space for allocation of 13 cameras, with one of them having double the size.

It's possible to join as many quadrants as necessary as long as the final area is a rectangle.
To undo this joining, repeat the process with the right button of the mouse.

After creating the screenstyle, it will already be available in the Surveillance Client. To learn how to use it, consult the manual of the Surveillance Client.

© 2002 - 2011 by Digifort, all rights reserved

Chapter



17 IP Filters

As one more means of security, Digifort offers another tool which is extremely important for the security of the Digifort server – the IP filters.

These filters act like a firewall, blocking unwanted connections to the server.
IPs that will or will not have access to the systems can be added to the IP filters.

When a user tries to connect to the server by way of a blocked IP address, its connection will not be permitted, disconnecting it and registering the action in the log.

If this configuration is not done, all IPs are free to access the server.

17.1 How to access IP Filters

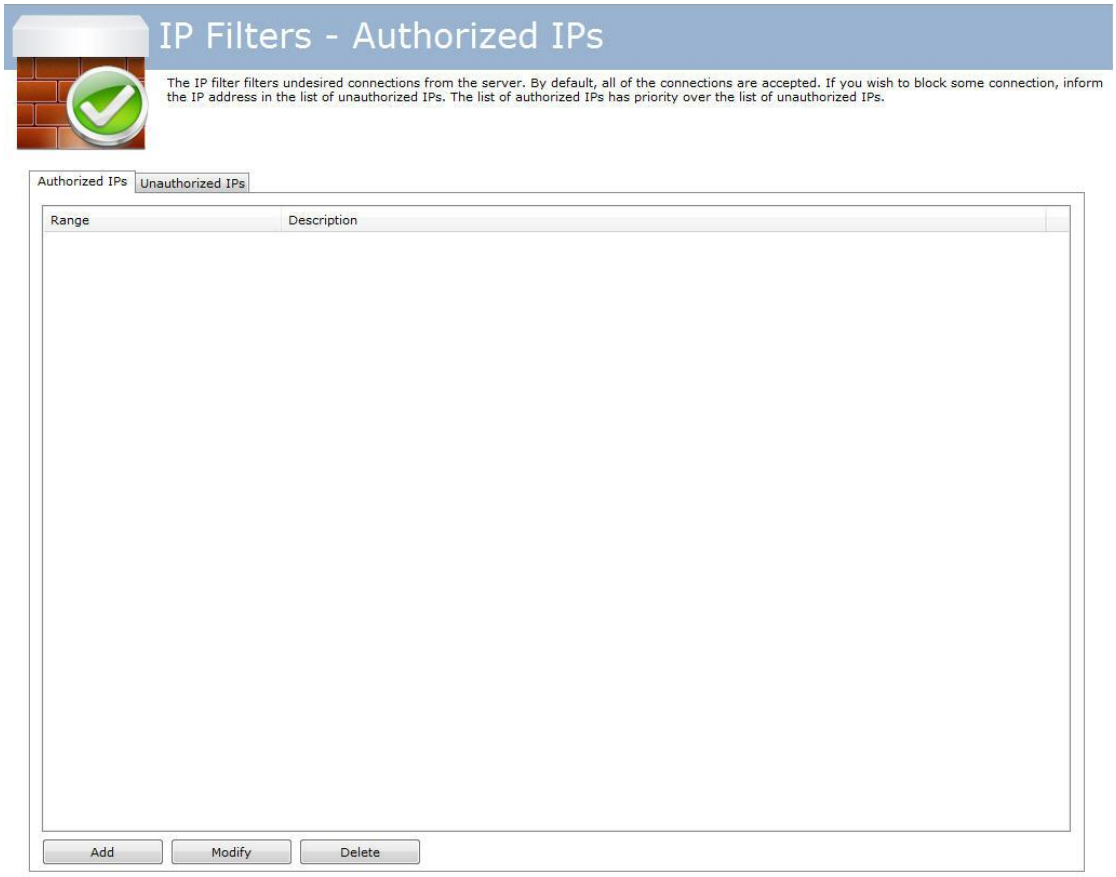
To access the IP filters, locate the item IP Filters in the Configurations Menu, as shown in the picture below:



Once this is done, the IP filters register will be displayed at the right, as shown in the picture below:
This configuration is divided into two parts: authorized IPs and unauthorized IPs. The authorized IPs are more privileged than the unauthorized ones, that is, if a given authorized IP is in the range of unauthorized IPs, it will be permitted.

In the examples given below, we will block all IPs and free only the surveillance stations:

© 2002 - 2011 by Optiview USA all rights


IP Filters - Authorized IPs
The IP filter filters undesired connections from the server. By default, all of the connections are accepted. If you wish to block some connection, inform the IP address in the list of unauthorized IPs. The list of authorized IPs has priority over the list of unauthorized IPs.
Authorized IPs
Unauthorized IPs
Range
Description
Add
Modify
Delete

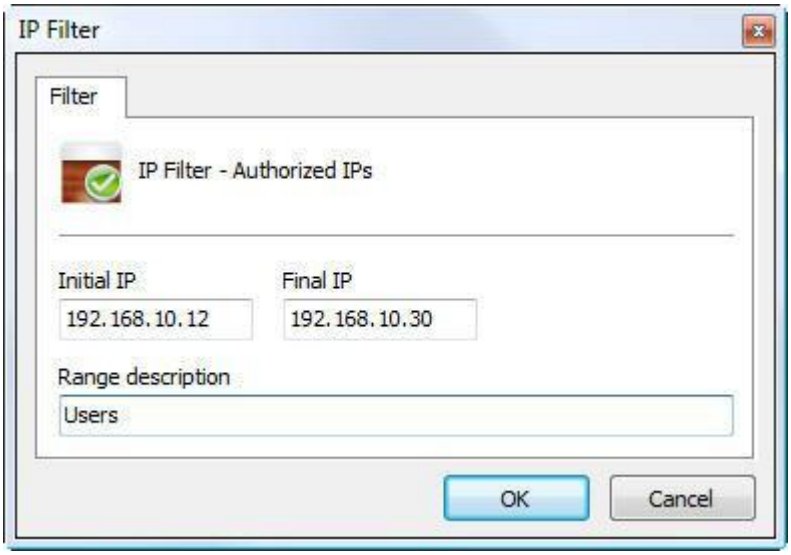
In the example in the picture above the IPs in the range from 192.168.10.12 to 192.168.10.30 are free for access to the server.

To add authorized IPs, click on **Add**. To modify or exclude authorized IPs, select it and click on the corresponding button.

17.1.1 How to add authorized IPs

After clicking on **Add**, as explained in the previous topic, the screen below will be displayed:

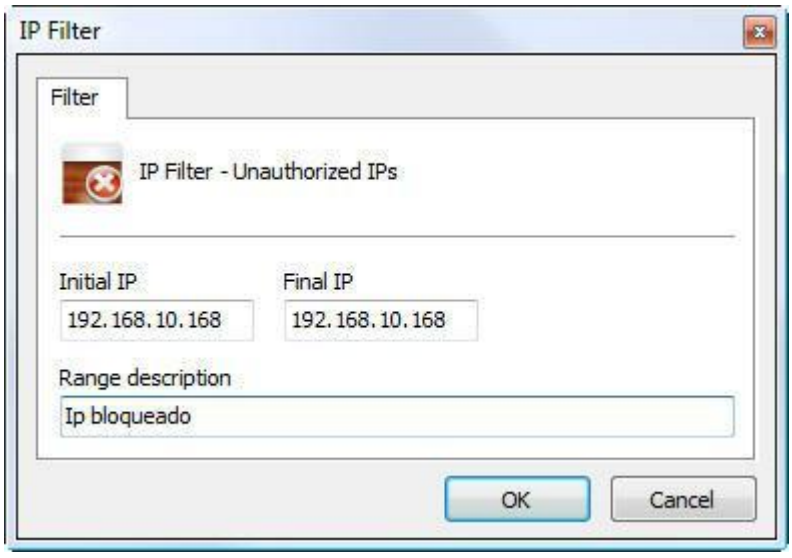
© 2002 - 2011 by Optiview USA all rights



- **Initial IP**: initial IP of the range to be configured.
- **Final IP**: final IP of the range to be configured.
- **Description of the range**: Identification name of the range to be configured.

17.1.2 How to add unauthorized IPs

To add unauthorized IPs, click on the Unauthorized IPs tab and then click on Add, opening the screen below:



- **Initial IP**: initial IP of the range to be configured.
- **Final IP**: final IP of the range to be configured.
- **Description of the range**: Identification name of the range to be configured.

© 2002 - 2011 by Optiview USA all rights

Chapter VII

18 Global Configurations

This area of the system is reserved for adjustment of the global configurations of the server.

Global configurations are parameter which, once configured, will affect the entire functioning of the system. afetarão todo o funcionamento do sistema.

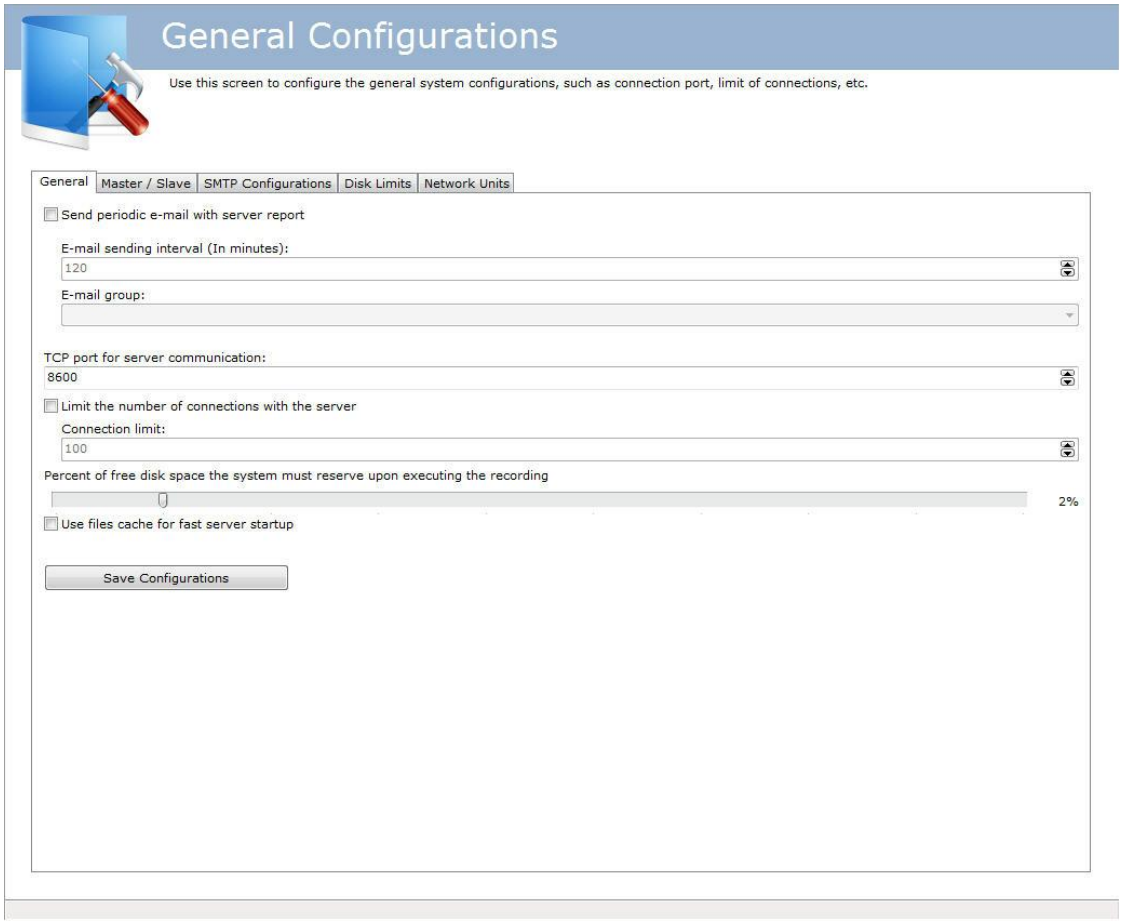
18.1 General Configurations

To access this area, click on the Configurations item in the Configurations Menu, as shown in the picture below:



Once this is done, the general system configurations screen will be opened at the right, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights


General Configurations
Use this screen to configure the general system configurations, such as connection port, limit of connections, etc.
General
Master / Slave
SMTP Configurations
Disk Limits
Network Units
Send periodic e-mail with server report
E-mail sending interval (In minutes):
120
E-mail group:
TCP port for server communication:
8600
Limit the number of connections with the server
Connection limit:
100
Percent of free disk space the system must reserve upon executing the recording
2%
Use files cache for fast server startup
Save Configurations

- **Send periodic e-mail with server report:** Sends e-mail with a server report periodically to the specified alert group in the specified time interval. This report contains information such as user accesses to the system and recording status.
- **TCP communication port with the server:** Communication port by which the Surveillance Client and the Administration Client will communicate with the server. After modifying this configuration, it's necessary to modify the communication port of the server register of the Administration Client and the Surveillance Client. To learn how to carry out this configuration in the Surveillance Client, see How to configure the servers to be administrated. To learn how to modify the port in the Surveillance Client, consult its manual..
- **Limit the number of connections with the server**: Limits the number of connections with the server. This value must be informed very carefully, as the number of connections opened with the server does not mean the number of logged-on users, but rather the number of connections established with the server and the cameras. For example, if a user is in the surveillance client, visualizing four cameras at the same time, then five connections with the server are made, one connection of the surveillance client and four other connections with the cameras.
- **Percentage of free disk space that the system must maintain while recording**: Enter here the percentage of disk space that you want to reserve for application softwares other than Digifort. For example, if an 80GB rigid disk is used, with 2% of free space, 16GB will not be used by Digifort for recordings, this being directed to other software, such as the operating system. This limit is also applied in "Disk limits". To learn how to create a disk limit, see Disk Limits

© 2002 - 2011 by Optiview USA all rights

After adjusting the configurations, click on the Save Configurations button so that no modification is lost.

Important

The percentage of free disk space reserves a disk space for application software other than Digifort. As default, it's configured with 2%. If you have a lot of space available in disk for recordings, maybe this value is very high.

18.2 Master / Slave

The master / slave option was developed in case there is more than one server with Digifort that needs to share user information, user groups, contacts, contact groups, and screen styles.

The server by default is always **Master**. To be configured as **Slave** simply select the 'slave' option and fill in the fields as indicated below: The **Slave** server will import all the **Master** server configurations.



The screen has the following functionalities:

- **Master server address:** The master server's IP address or server DNS from where the user information, user groups, contacts, contact groups and alerts will be replicated.
- **Password of the master server's admin user**: Password of the admin user for server access.

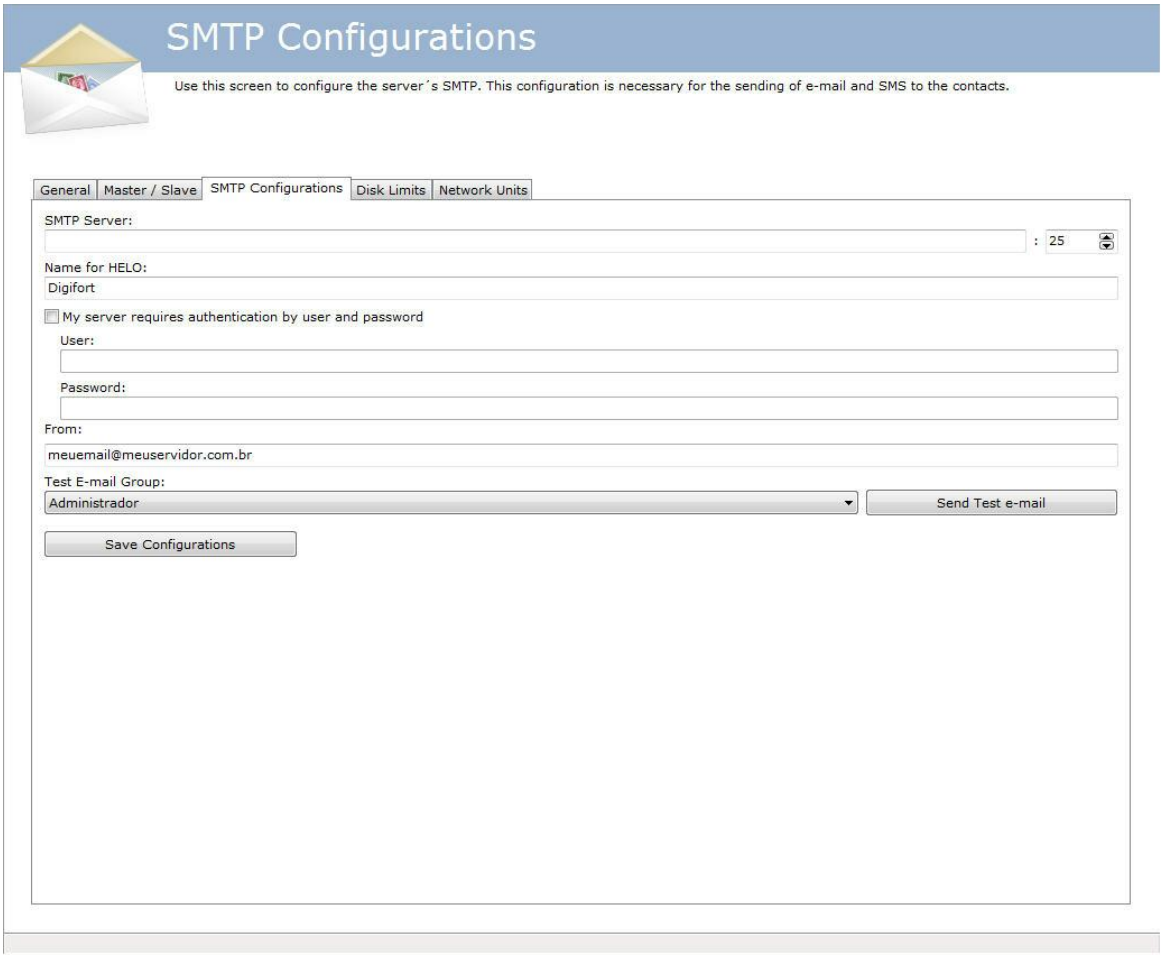
To apply all configurations, click on **Save Configurations**. You'll see that all the information was successfully exported.

18.3 STMP Configurations

The STMP configurations are used by Digifort t send notification e-mail to users. The actions for sending e-mail could be failures in communication with the cameras, for example, and must be previously configured by the administrator.

To access this feature, click on the **STMP Configurations** tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



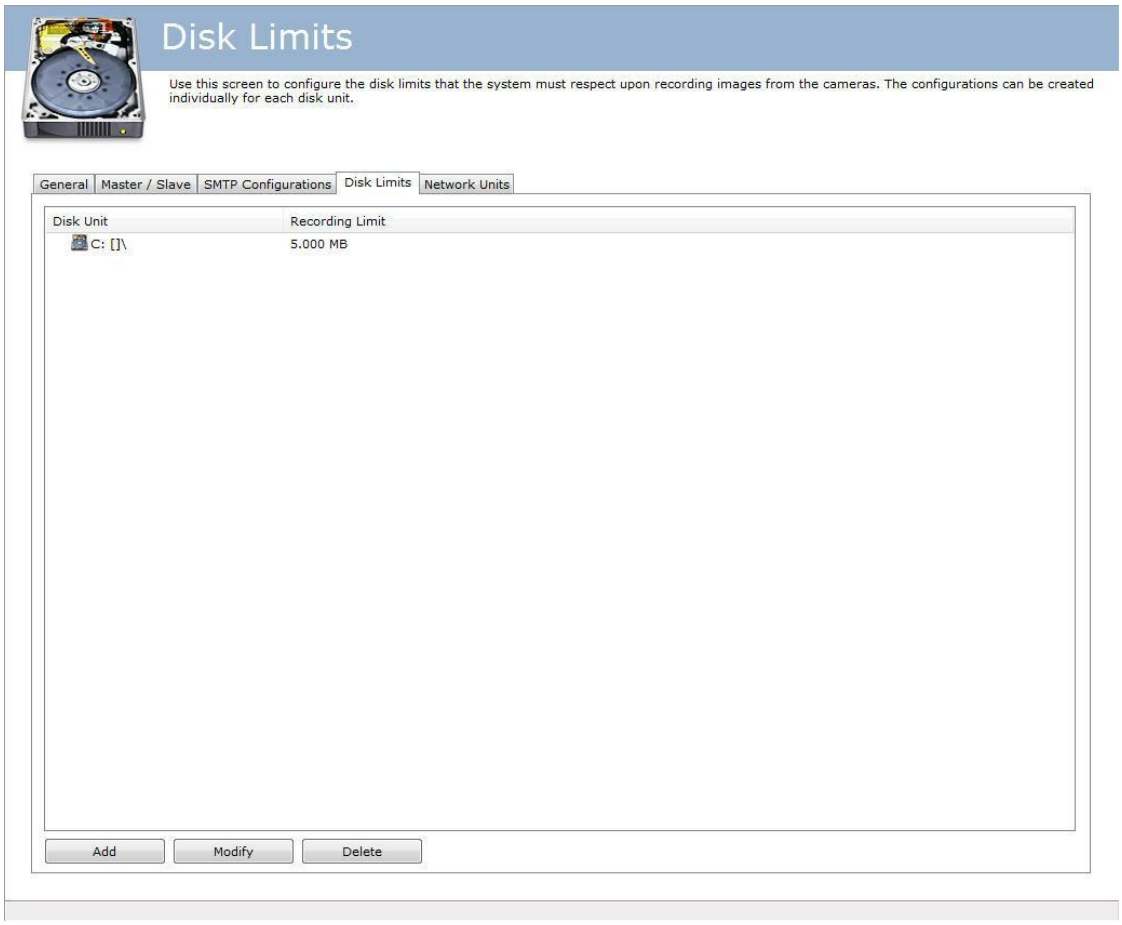
- **STMP Server SMTP**: Address of the SMTP server to be used for the sending of e-mail. This parameter can be an IP, if there is an STMP server in your company, for example, or a DNS if third-party STMP servers are used.
- **My server needs authentication by user and password:** If your SMTP server needs a user and password for authentication for sending of e-mail, mark this option. When this option is marked, the User and Password fields will be activated and must be filled in.
  - **User:** User for authentication in the sending of e-mail messages.
  - **Password**: Password for authentication in the sending of e-mail messages.
- **From:** Sender's e-mail address. In this field, enter the e-mail address of the system administrator, for example.
- **Group for test e-mail**: Select an alert group for the sending of a test e-mail message for the specified configurations. This alert group must have been previously configured. To learn how to do this configuration see How to configure the contact groups
- **Save Configurations button:** Saves the configurations. If not pressed, no configurations will be saved after leaving this screen.

18.4 Disk Limits

In this area of the system you can define disk limits in all of your units, if you wish to maintain a cushion of free disk space.

© 2002 - 2011 by Optiview USA all rights

To access this feature, click on the Disk Limits tab in the Configurations item of the Configurations Menu, as shown in the picture below:



To add a disk limit, click on the **Add** button.

© 2002 - 2011 by Optiview USA all rights


Global Disk Limit
Global Disk Limit
Configurations of Global Disk Limit
With the global disk limit configurations you can restrict the use of HD for the recording of cameras configured to record with limit of recording by hours or days.
Select the disk to impose a Recording Limit
C: []\ (238.464 MB)
Supply a Recording Limit (In MB)
5000
OK
Cancel

Select the desired disk unit and enter the number of megabytes of limit that you wish to impose.
At the end of the configuration, click on the **OK** button.

To remove a disk limit, select it and click on the **Remove** button.

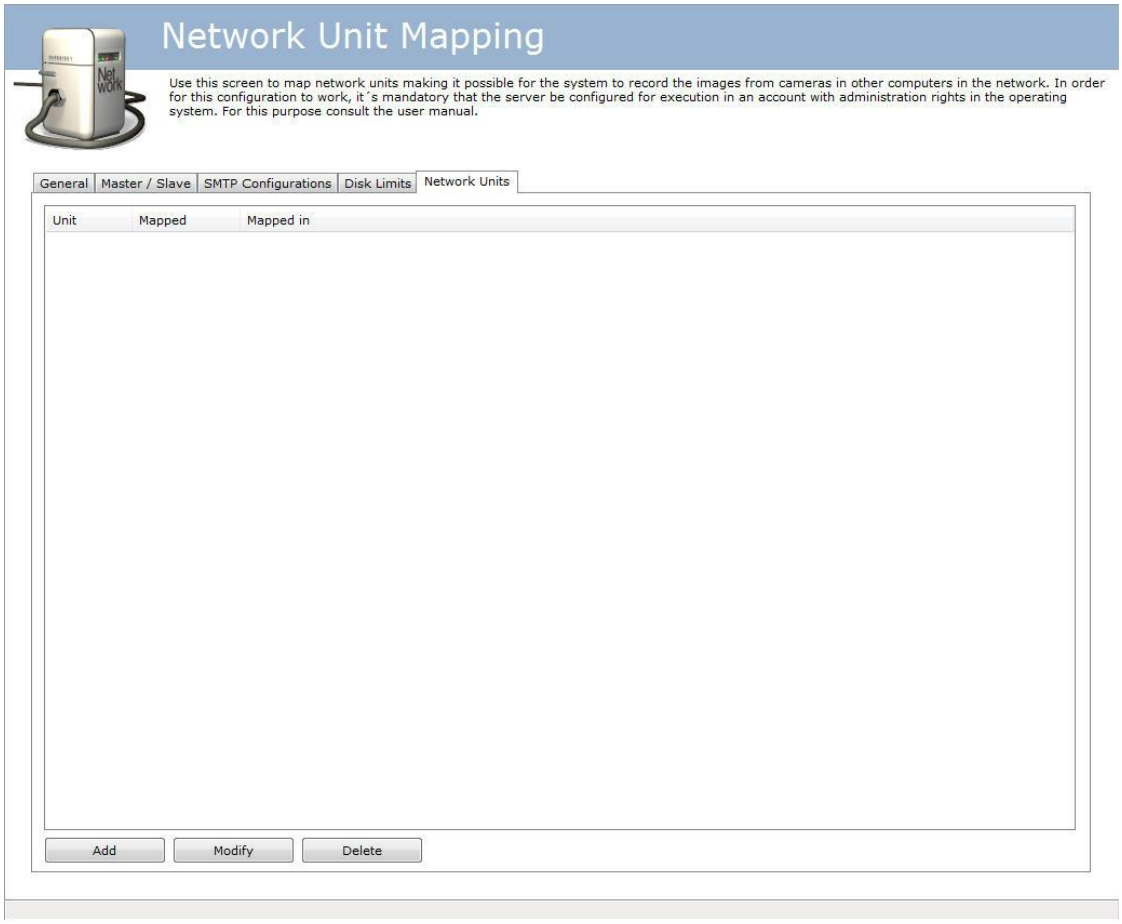
18.5 Network Units

Digifort Enterprise makes it possible to carry out recording of cameras not only in local disks. It's also possible to define network units in which Digifort can record the images from cameras.

Digifort's mapping of network units is different from that of Windows, and must, therefore, be defined by Digifort itself.

To access this feature, click on the **Network Units** tab, as shown in the picture below::

© 2002 - 2011 by Optiview USA all rights

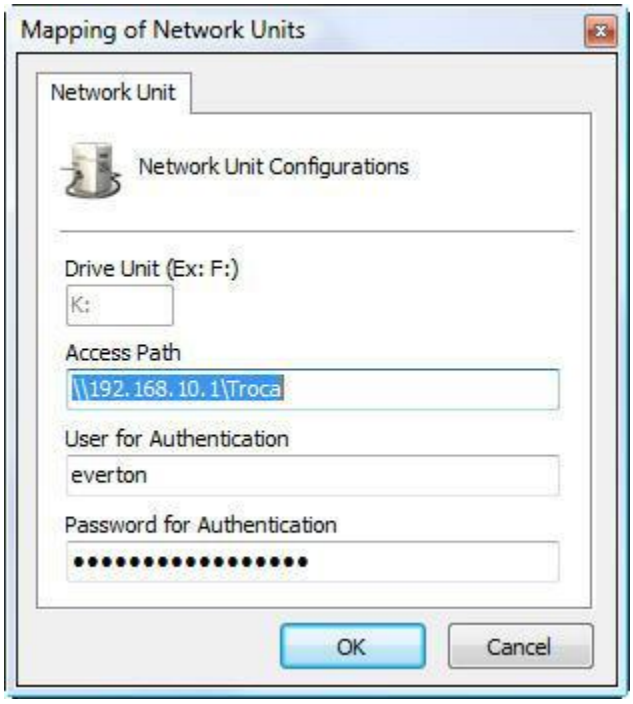

Network Unit Mapping
Use this screen to map network units making it possible for the system to record the images from cameras in other computers in the network. In order for this configuration to work, it´s mandatory that the server be configured for execution in an account with administration rights in the operating system. For this purpose consult the user manual.
General
Master / Slave
SMTP Configurations
Disk Limits
Network Units
Unit
Mapped
Mapped in
Add
Modify
Delete

To add a new network unit, click on **Add**. To modify or exclude a network unit, select it and click on the corresponding button.

18.5.1 How to add a network unit

After clicking on **Add**, as explained in the previous topic, the following screen will be displayed:

© 2002 - 2011 by Optiview USA all rights



- **Unit letter**: Specify the identification letter of the unit to be mapped.
- **Access path**: Specify the complete folder path of the unit to be mapped.
- **User for authentication**: User of the Windows network who has access to the folder.
- **Password for authentication**: Password of the Windows network who has access to the folder.

© 2002 - 2011 by Optiview USA all rights

© 2002 - 2011 by Optiview USA all rights

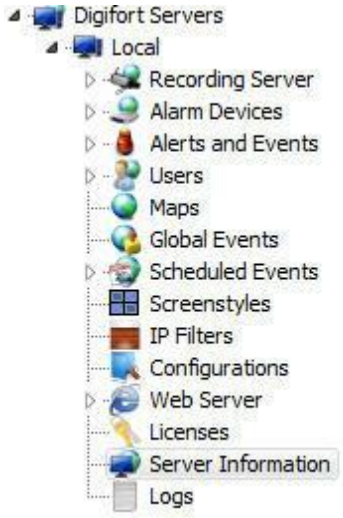
Chapter



19 Server Information

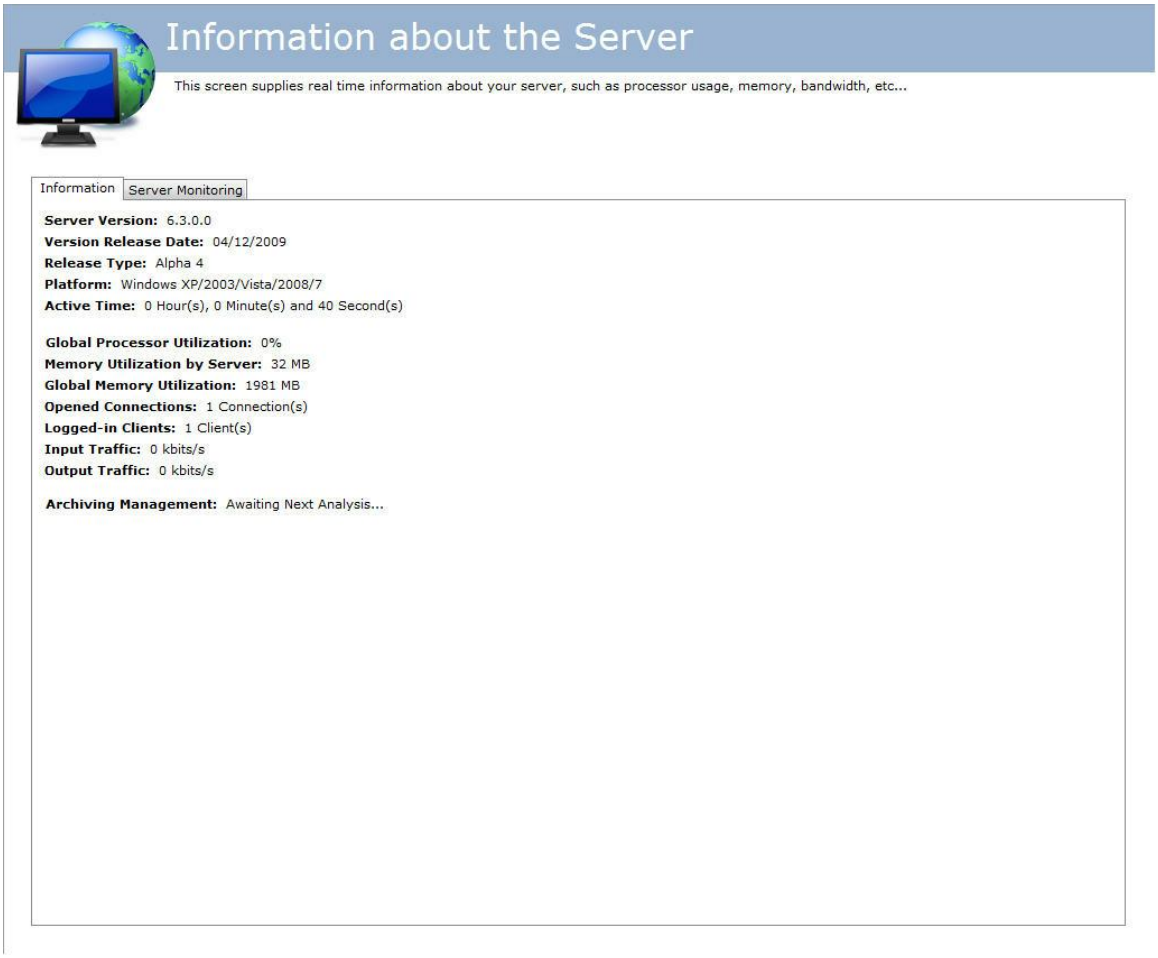
In this area of the system you will be able to accompany the performance of the server, receiving data such as processor and memory utilization, network traffic, etc.

To access this feature, click on the **Server Information** item in the Configurations Menu, as shown in the picture below:



Once this is done, a window will be opened on the right side with server information, as shown in the picture below:

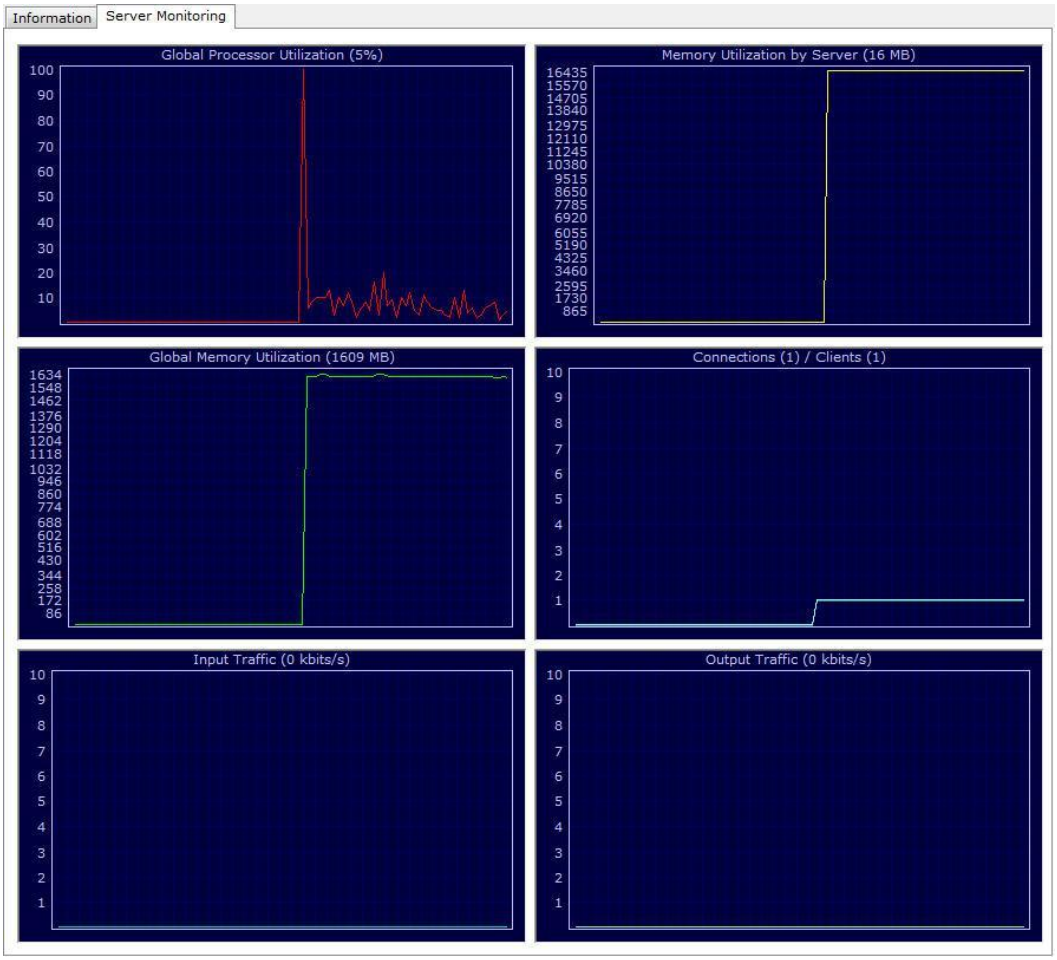
© 2002 - 2011 by Optiview USA all rights


Information about the Server
This screen supplies real time information about your server, such as processor usage, memory, bandwidth, etc...
Information
Server Monitoring
Server Version: 6.3.0.0
Version Release Date: 04/12/2009
Release Type: Alpha 4
Platform: Windows XP/2003/Vista/2008/7
Active Time: 0 Hour(s), 0 Minute(s) and 40 Second(s)
Global Processor Utilization: 0%
Memory Utilization by Server: 32 MB
Global Memory Utilization: 1981 MB
Opened Connections: 1 Connection(s)
Logged-in Clients: 1 Client(s)
Input Traffic: 0 kbits/s
Output Traffic: 0 kbits/s
Archiving Management: Awaiting Next Analysis...

19.1 Monitoring by graphics

Digifort offers an interesting feature that makes it possible to monitor the resources used by the server in real time by way of graphics updated every second. To access this configuration, click on the **Monitoring** tab, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



© 2002 - 2011 by Optiview USA all rights

Chapter



20 System Logs

The logs are very important tools for an environment that involves a security system such as Digifort, as it is in these logs that all events are registered, as well as user actions that occur in the system.

This chapter of the manual will cover the system logs, that is, those in which server events are registered, as opposed to the logs of alerts and events, where events related to external devices are registered. To better understand what alert and event logs are, see How to access the Alerts and Events

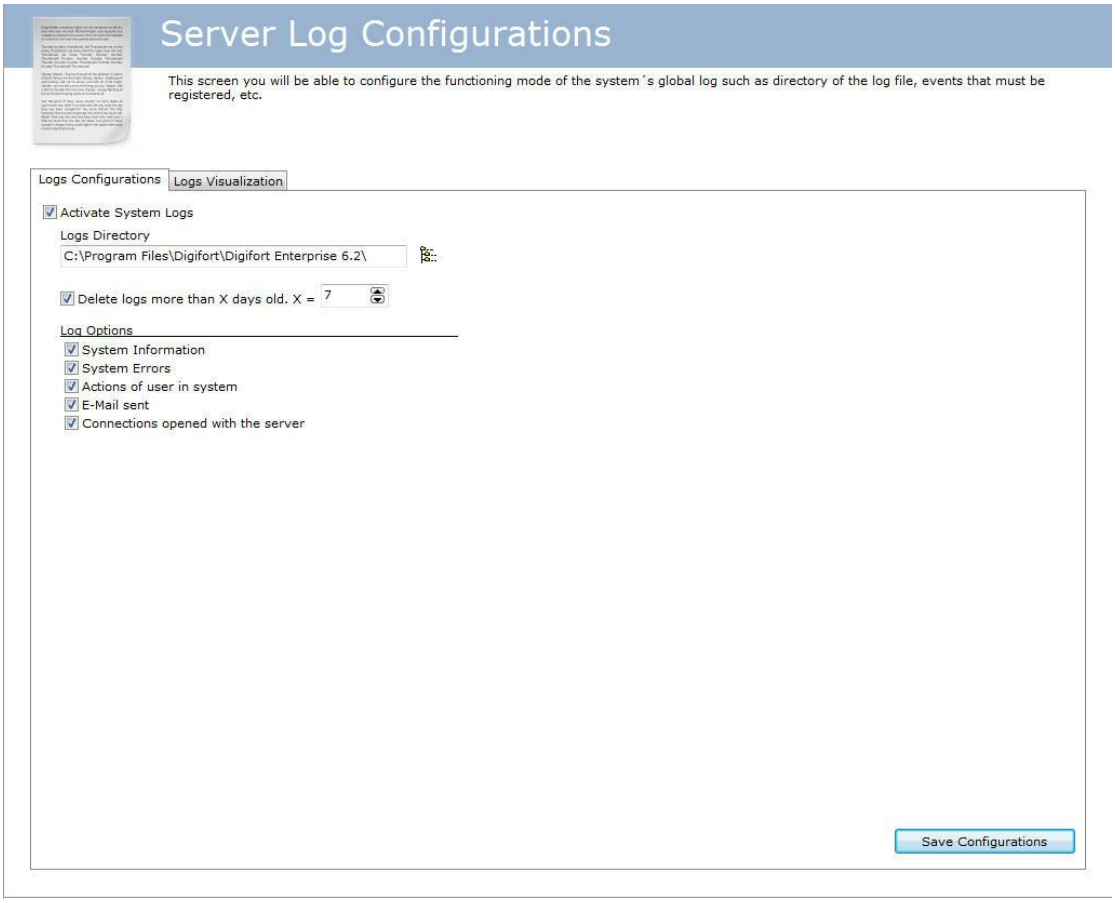
20.1 How to access the system logs

To access the system logs, click on the Logs item, located in the Configurations Menu, as shown in the picture below:



Once this is done, the configuration of logs will be displayed on the right, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights


Server Log Configurations
This screen you will be able to configure the functioning mode of the system´s global log such as directory of the log file, events that must be registered, etc.
Logs Configurations
Logs Visualization
Activate System Logs
Logs Directory
C:\Program Files\Digifort\Digifort Enterprise 6.2\
Delete logs more than X days old. X =
7
Log Options
System Information
System Errors
Actions of user in system
E-Mail sent
Connections opened with the server
Save Configurations

- **Activate system logs**: Activates the alert and event logs of Digifort.
- **Log directory**: Select the directory in which the alert and event logs will be saved.
- **Eliminate logs more than X days old**: Eliminates the old logs, specified by the informed number of days.

- **Options of the event log:**
  - **System information**: This log contains information about system functioning like, for example, the time at which the server was loaded, terminated.
  - **System errors**: This log contains information about system errors such as the incorrect execution of some system function. This log rarely receives data.
  - **System user actions:** This log contains information about system user actions like, for example, the visualization of some camera and modification of configurations.
  - **E-mail sent:** This log contains information about the e-mail messages sent by Digifort like, for example, e-mail messages about failures in recording or communication of cameras.
  - **Open connections with the server:** This log contains information about the user connection with the server, showing information such as access time and IP.
- **Save Configurations button:** Saves the configurations of system logs.

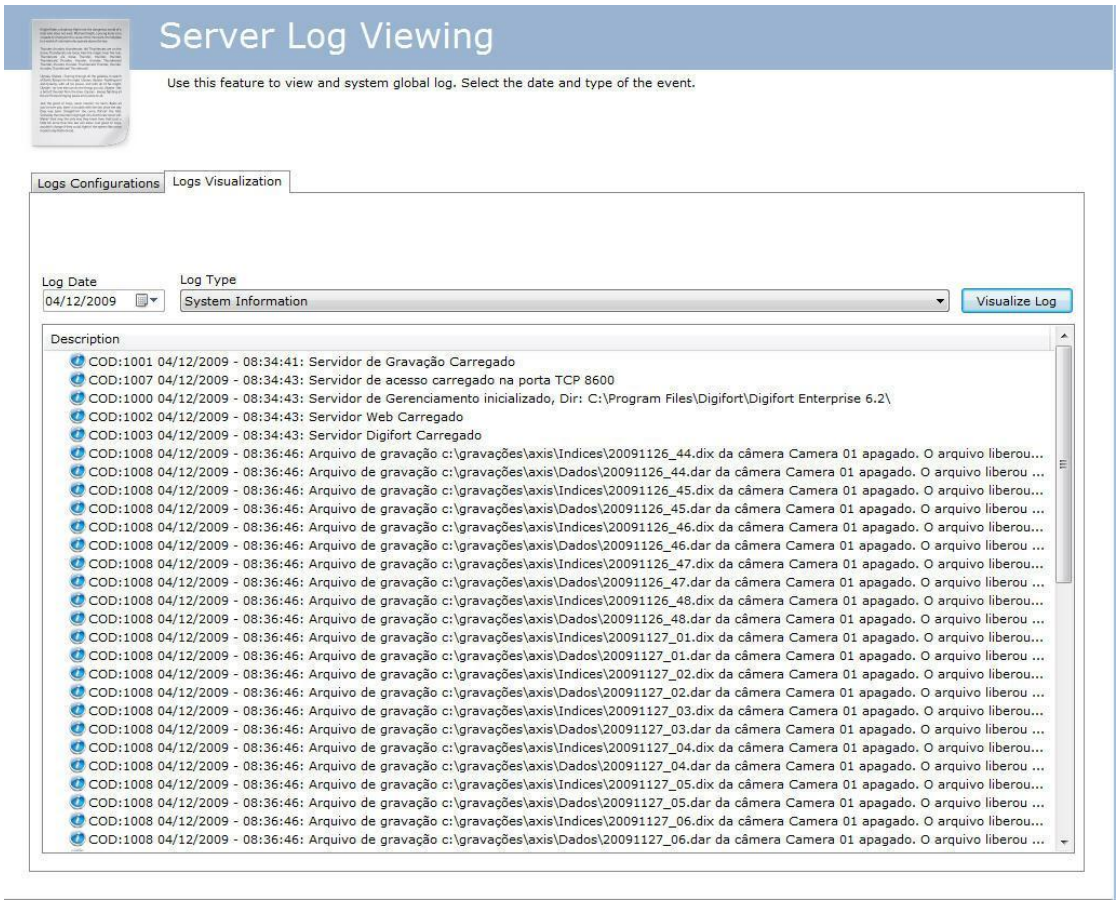
20.2 How to visualize the event logs

The visualization of logs is an auxiliary tool for the administrator when analyzing a log,

© 2002 - 2011 by Optiview USA all rights

presenting a friendlier and more productive interface compared to a simple text file.

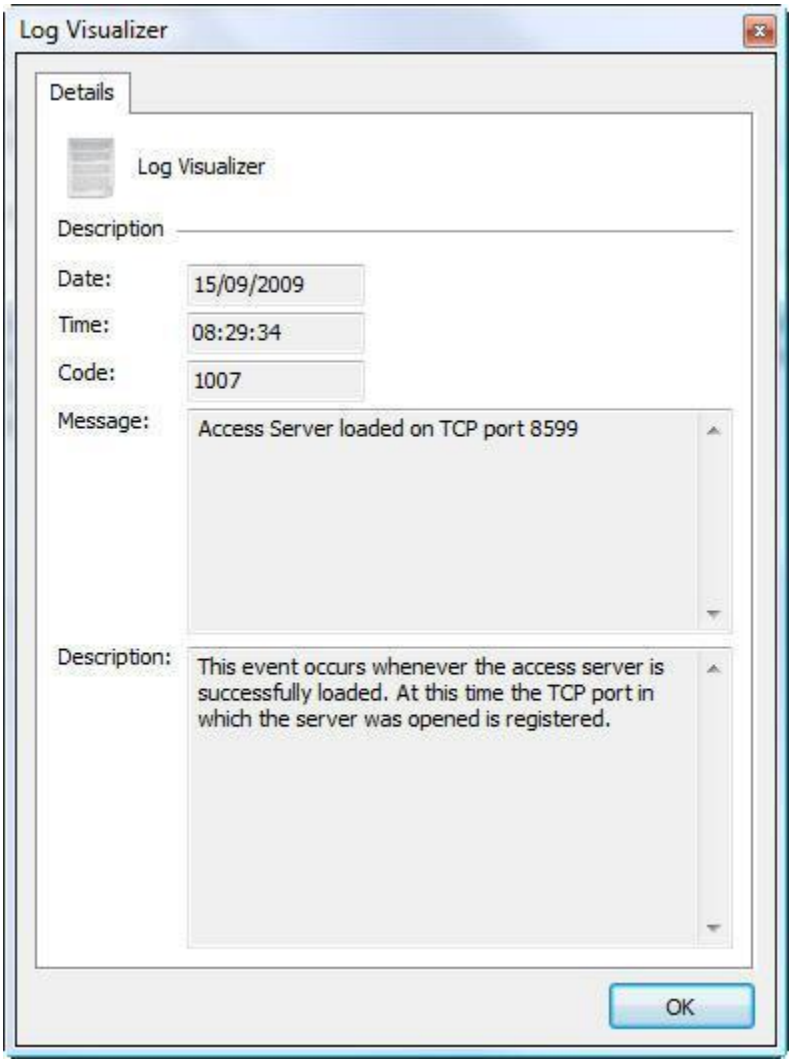
To visualize the event logs, click on the **Log visualization** tab, as shown in the picture below:



To visualize a log, select the date and type, then click on the Visualize Log button. This way the list of log registers will be filled.

Upon double-clicking on some log item, a screen will be displayed with details about the occurrence, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



© 2002 - 2011 by Optiview USA all rights

Chapter



21 Web Server

Digifort is equipped with a Web server, by means of which, users can visualize cameras and play videos back locally or via Internet with the use of an Internet navigator.

It's important to point out that, for access to the Digifort Server via Internet, it's necessary to configure your router with the purpose of redirecting the server connection by way of an Internet IP and a port.

To carry out the connection via Internet, Digifort requires two communication ports, the port 8600 and another configurable port.

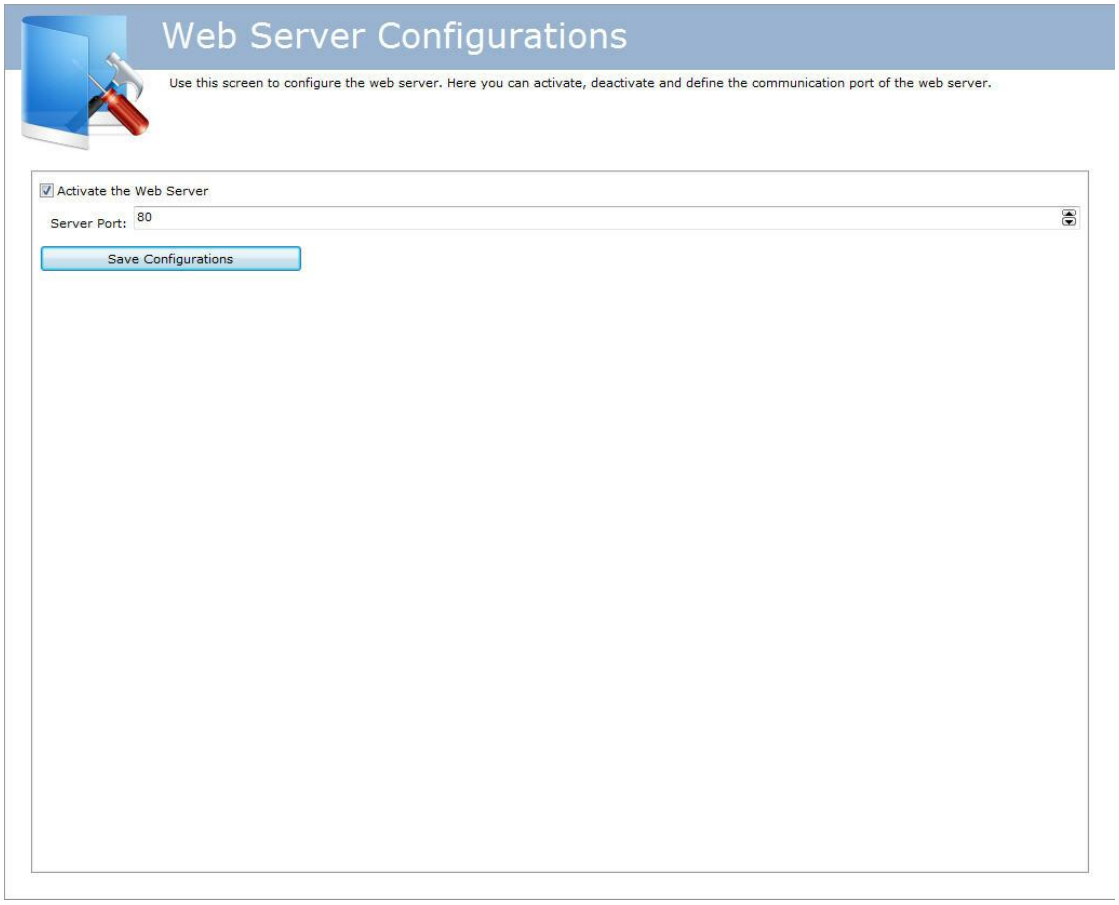
21.1 How to access the configurations of the Web Server

To access the configurations of the Web Server, click on the item **Web Server**, and click on **Configurations**, located in the Configurations Menu, as shown in the picture below:



Once this is done, the configurations of the Web Server will be displayed at right, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights


Web Server Configurations
Use this screen to configure the web server. Here you can activate, deactivate and define the communication port of the web server.
Activate the Web Server
Server Port:
80
Save Configurations

- **Activate the Web server**: Activates the Web server Web allowing users to connect to the server by way on an Internet navigator.
- **Server port:** The port used for access to the server. This port can be modified and must be configured in your router for external access. Digifort uses a different one internally, because the port 8600

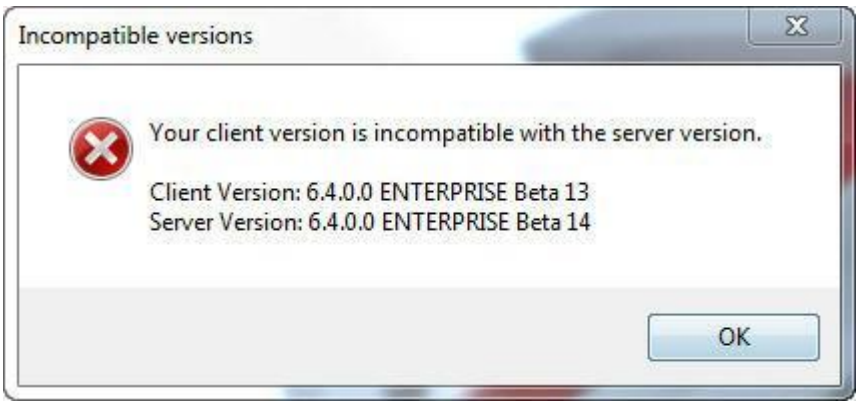
© 2002 - 2011 by Optiview USA all rights

Chapter XXII

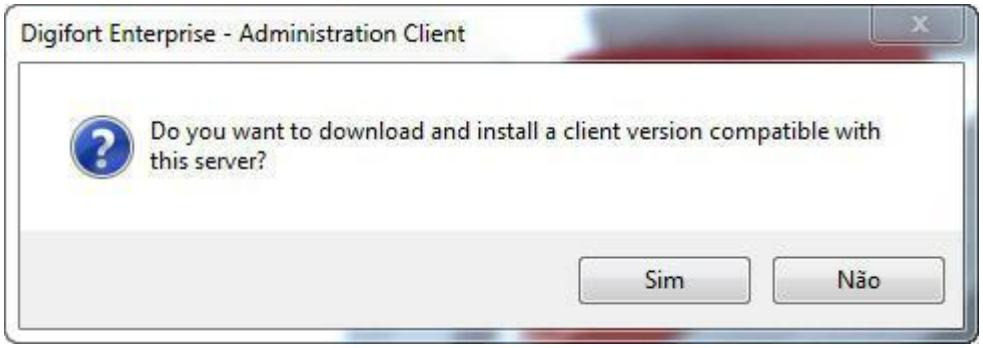
22 Automatic Client update

With swiftness and speed in mind, Digifort created a new feature that will be available in all the post-6.4 versions: the automatic update of the Surveillance and Administration Clients.
The feature will check if the server versions to which the client is trying to connect are the same.

When logging into the system, whether at the Administration Client or the Surveillance Client, if the versions are not compatible (for example: 6.4 with 6.5) the following message will appear: **Your client version is incompatible with the server version**, as shown in the picture below:


Incompatible versions
Your client version is incompatible with the server version.
Client Version: 6.4.0.0 ENTERPRISE Beta 13
Server Version: 6.4.0.0 ENTERPRISE Beta 14
OK

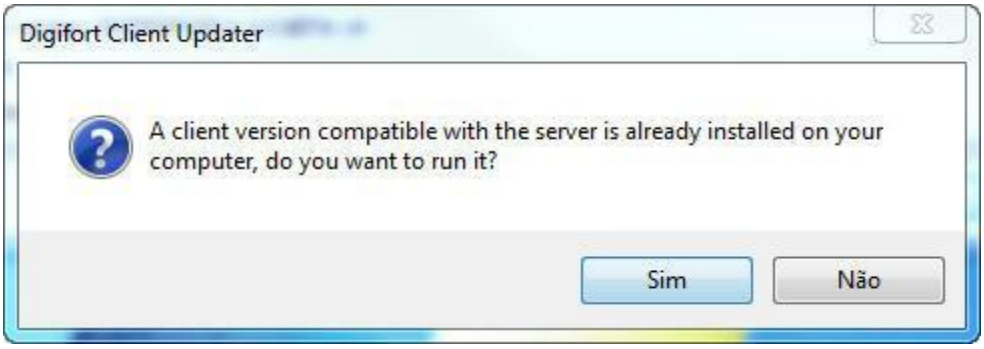
By clicking on **OK** a dialogue box will open with the following question: **Do you wish to download and install a client version compatible with this server?**


Digifort Enterprise - Administration Client
Do you want to download and install a client version compatible with this server?
Sim
Não

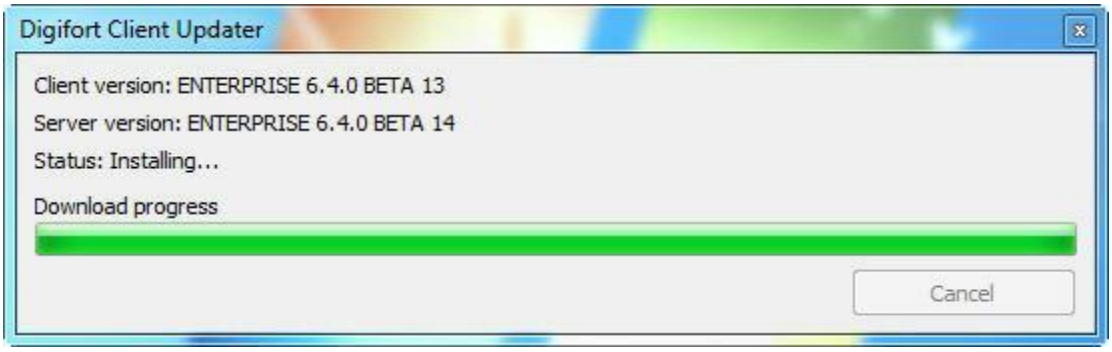
If you click on **No** the dialogue box closes and nothing happens. If you click on **Yes**, Digifort automatically installs the compatible client versions on the computer.

If the Digifort version on your computer is compatible, you will get the following message: **A compatible version is already installed on your computer; do you wish to execute it?**

© 2002 - 2011 by Optiview USA all rights

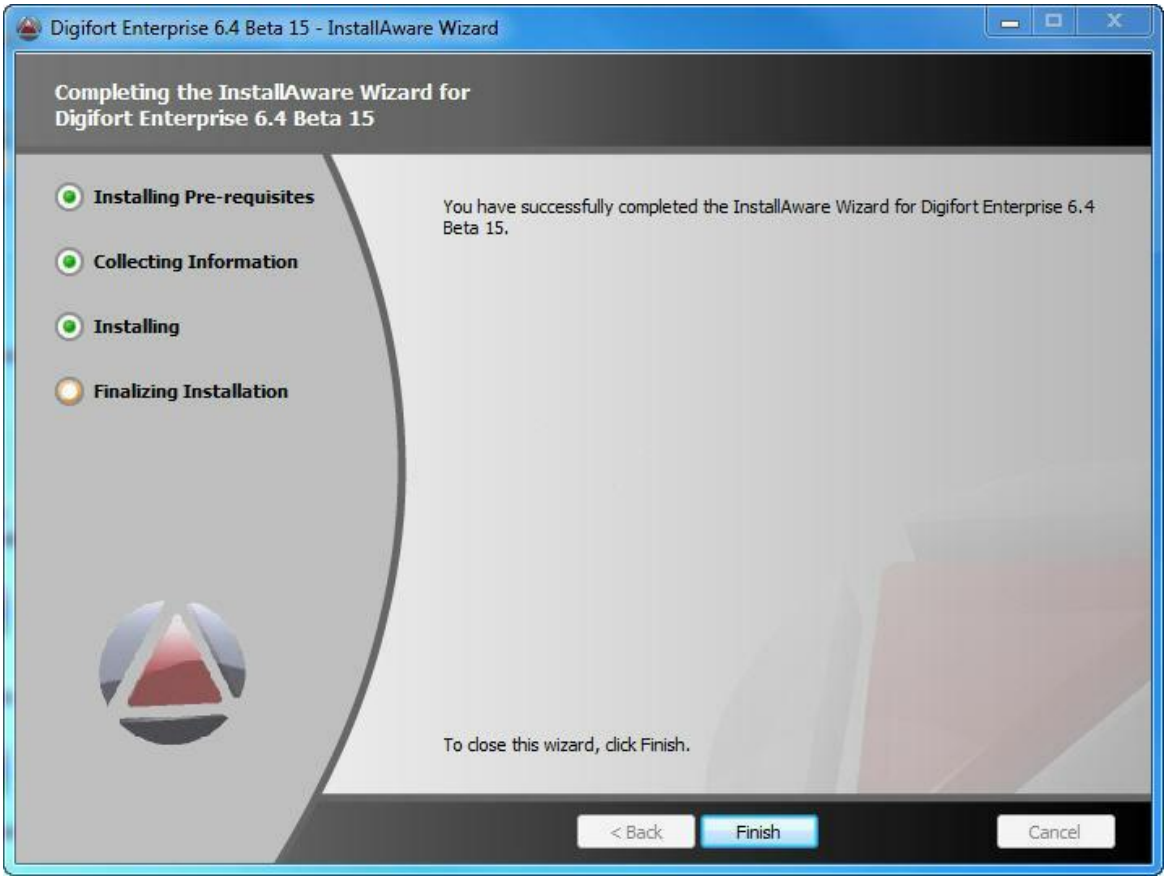

Digifort Client Updater
A client version compatible with the server is already installed on your computer, do you want to run it?
Sim
Não

If you click on **Yes** the client will execute. Otherwise, the client installation will continue:



Continue the installation as normal and at the end click on **Finish**:

© 2002 - 2011 by Optiview USA all rights


Digifort Enterprise 6.4 Beta 15 - InstallAware Wizard
Completing the InstallAware Wizard for Digifort Enterprise 6.4 Beta 15
Installing Pre-requisites
Collecting Information
Installing
Finalizing Installation
You have successfully completed the InstallAware Wizard for Digifort Enterprise 6.4 Beta 15.
To close this wizard, click Finish.
< Back
Finish
Cancel

Once installed, the compatible client is ready to connect to the requested server.

© 2002 - 2011 by Optiview USA all rights

Chapter XII

23 Failover

The Digifort servers can be configured to work with Failover, that is, another server will take over if one stops working.

For information purposes, let's imagine a company with two Digifort servers, **server A** with 4 cameras, and server B as FailOver. If **server A** fails, **server B** will start recording from the 4 cameras.

This feature will only work if both servers are licensed and if **server B** has an extra license (one more than **server A)**. **Server B**'s extra license will trigger the event for all the others to start recording.

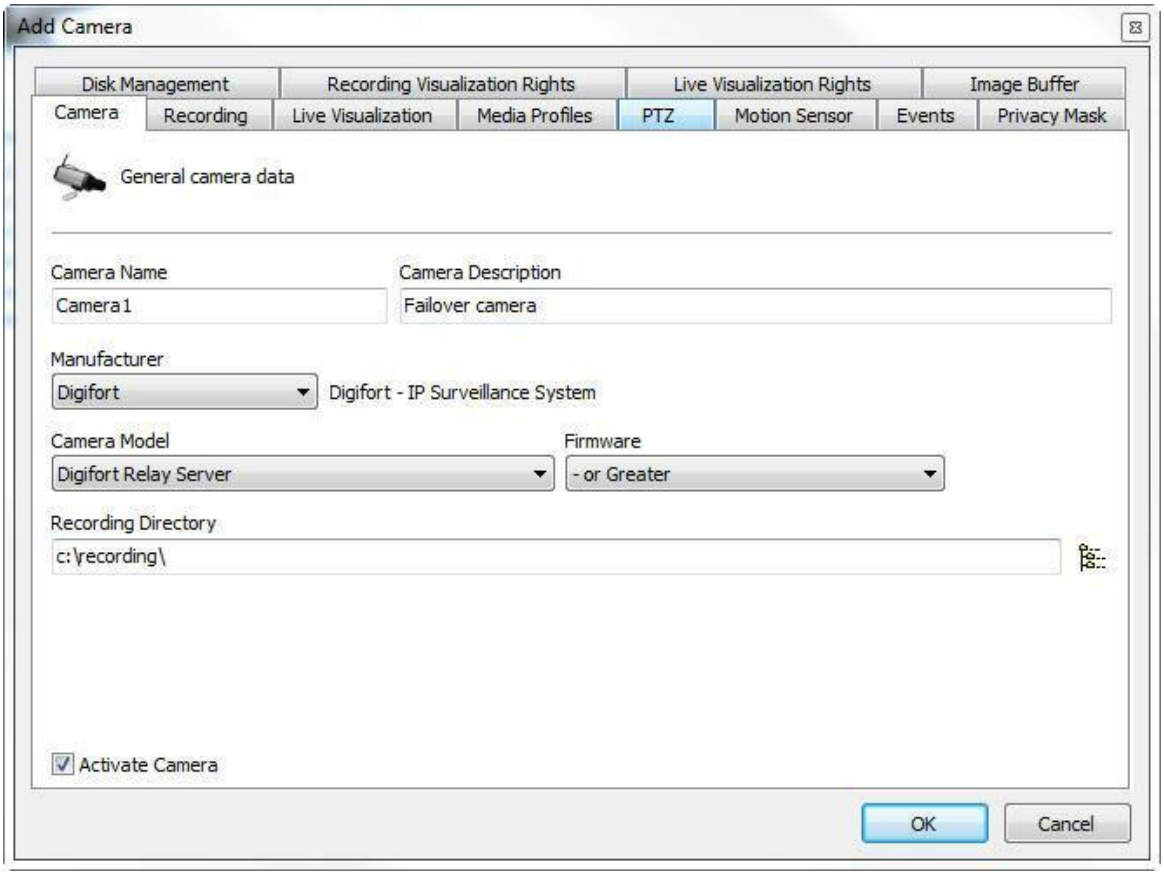
23.1 Configuring the Failover server

First of all, **server A** must be configured with all 4 cameras functioning. Then, in **Server B**, register all the cameras again.

Now, in server B, configure the camera that will trigger the event for the others to start recording.

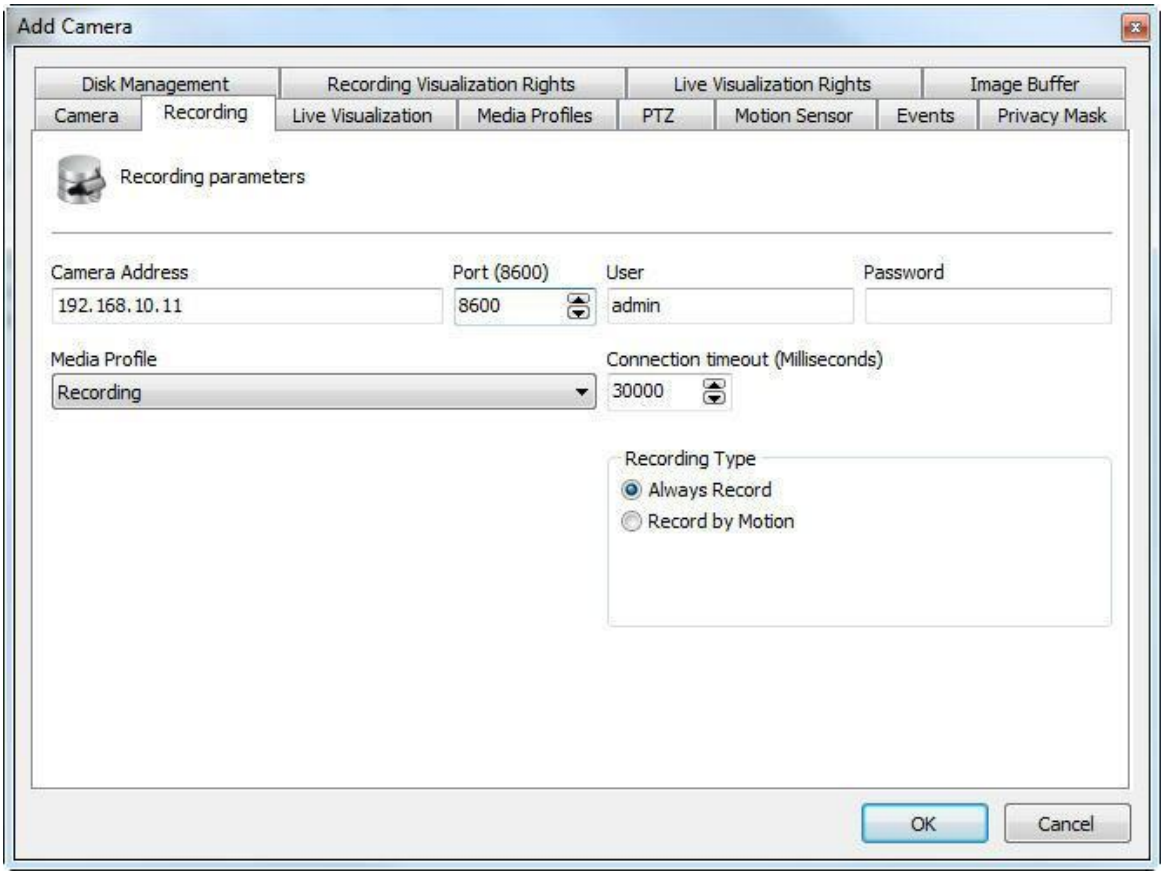
Add another camera. Under 'manufacturer' choose **Digifort**, and under 'model' choose **Digifort Relay Server** as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



This configuration will register the camera with the name "**Camera1**" of **Server A** in Server B. Now you must configure **server A**'s IP. That configuration is made in the **Recording** tab:

© 2002 - 2011 by Optiview USA all rights

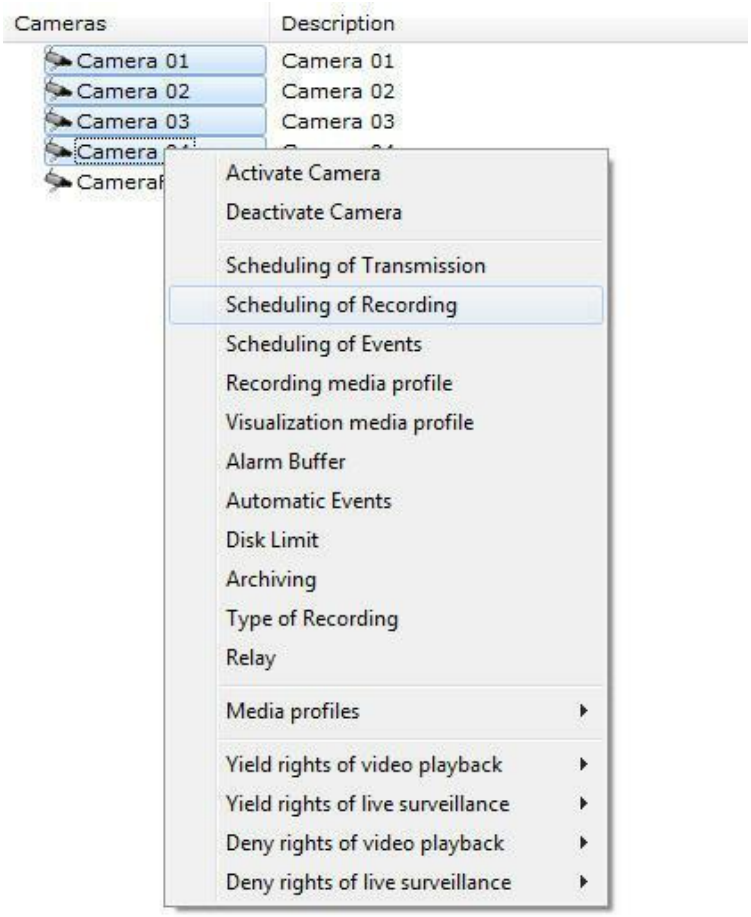


The port will be configured to be Digifort server's port, in this case, port **8600**.

Once the **Failover camera** has been registered and is working, you can configure all the other cameras in that server (**server B**) so that they may start recording if there is failure in communication.

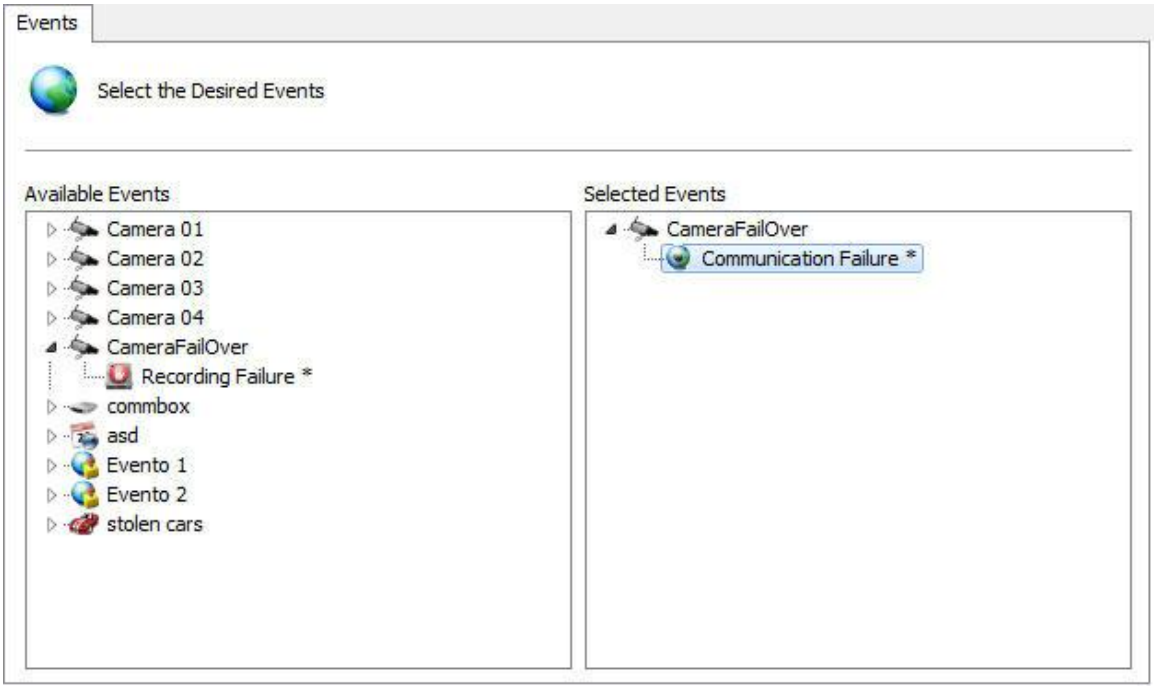
Click with the right-hand button on all the **Server B** cameras, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



And then click on **Schedule Recording**. In the schedule recording, choose the **failure in communication** of the Failover camera as the event to start recording, as shown in the picture below:

© 2002 - 2011 by Optiview USA all rights



In other words, when the failover camera has a **failure in communication** it means **Server A** is not working and **server B** will start recording for all the other cameras.

Once the problems have been stabilized with the **main server (Server A)**, restart Digifort's service on the Failover server **(Server B)** so that the cameras can stop recording.

CONTACT INFORMATION

Sales:	904-805-1581
Licensing & Tech. Support	904-855-1121
Email	Sales@optiviewusa.com
Internet	http://www.OptiviewUSA.com

© 2002 - 2011 by Optiview USA all rights